GSA

Michael Gelber - PD <michael.gelber@gsa.gov>

Fwd: Get-Backs from the Sept. 9 Hearing

1 message

Alice Yates - S <alice.yates@gsa.gov> Tue, Nov 29, 2016 at 3:07 PM
To: Michael Gelber - PD <michael.gelber@gsa.gov>, Andrew Blaylock - OCIA <andrew.blaylock@gsa.gov>

Below are follow-up answers from the Sept. 9 hearing, provided to committee staff.

---------- Forwarded message ----------
From: **Ding, Michael** <Michael.Ding@mail.house.gov>
Date: Thu, Nov 17, 2016 at 6:01 PM
Subject: RE: Get-Backs from the Sept. 9 Hearing
To: Alice Yates - S <alice.yates@gsa.gov>
Cc: Dawne Troupe - 2A <dawne.troupe@gsa.gov>

Thank you!

From: Alice Yates - S [mailto:alice.yates@gsa.gov]
Sent: Thursday, November 17, 2016 5:13 PM
To: Ding, Michael
Cc: Dawne Troupe - 2A
Subject: Get-Backs from the Sept. 9 Hearing

Hi Michael,

Below are answers to questions from the Sept. 9 hearing. Please let us know if you have any additional questions. Thanks.

Status of the Coast Guard building in SW waterfront:

- The building the Coast Guard occupied (2100 2nd St. (Transpoint)) is no longer under GSA lease.
- After the USCG moved to St. E's, it was backfilled by NAVSEA after the Navy Yard shooting and then vacated prior to lease expiration (May 2015)
- Is GSA paying a lease on it? - No.
- When will the lease expire? It expired May, 2015.

FBI HQ Consolidation Project Update:

- Due to a strong and overwhelmingly positive response from developers to the solicitation issued earlier this year, the U.S. General Services Administration (GSA) and the Federal Bureau of Investigation (FBI) now plan to announce the selected site and offeror for the competition in early March 2017.
- GSA and FBI are encouraged by the proposals received and are confident that, if Congress provides the resources requested in the President's Fiscal Year 2017 budget, we will be able to deliver on our commitment to provide a world class facility for the FBI and a good deal for the taxpayer.

Potential Closure of the IRS Facility in Covington, Kentucky (Rep. Massie):

- The decision to close the Covington facility was announced by IRS Commissioner John Koskinen on September 14, 2016.

- The IRS has indicated the facility will close sometime after the end of the 2019 filing season, but sometime before the end of the fiscal year.

- GSA is working with the IRS on its requirements for the Covington area, which we believe will be finalized in the next year or so. After IRS finalizes its requirements, GSA will begin the analysis to determine if the federal building will be retained (and other federal leases moved into the building) or if the building is to go through the disposal process.

- As with any potential real estate repositioning, GSA would work with the community and your office concerning the repositioning and possible disposal of this federal asset.

- GSA has reached out to city and county officials to explain how a disposal process would move forward IF the building is disposed.

- We would be happy to meet with you or your staff to discuss further.

Herbert C. Hoover Building

- The U.S. General Services Administration (GSA) submitted a prospectus for the modernization of the Hoover Building as part of the Administration's Fiscal Year 2016 (FY2016) budget submission.

- This prospectus was identical to that submitted by GSA in Fiscal Year 2015 (FY2015).

- Neither of GSA's Congressional authorization committees in the House or Senate approved the prospectus for the Hoover modernization project in FY2015 or FY2016, and no appropriations were provided by Congress for this phase of the project.

- If GSA receives Congressional approvals and funding for the Hoover project, construction completion is expected in 2026, with occupancy in 2027.
- At that time, GSA expects that about 200,000 usable square feet (USF) would be available for occupancy by tenants other than those currently located in the building.
- GSA has not yet identified tenants for this space, and will be in a better position to assess which tenant agencies would best be suited for this location as this project progresses to its completion date.

Questions for The Honorable Alan Thomas
Commissioner
General Services Administration, Federal Acquisition Service

Questions for the Record from Chairman Mark Meadows Subcommittee on Government Operations
House Committee on Oversight and Government Reform

July 12, 2017, Hearing: "General Services Administration -Acquisition Oversight and Reform"

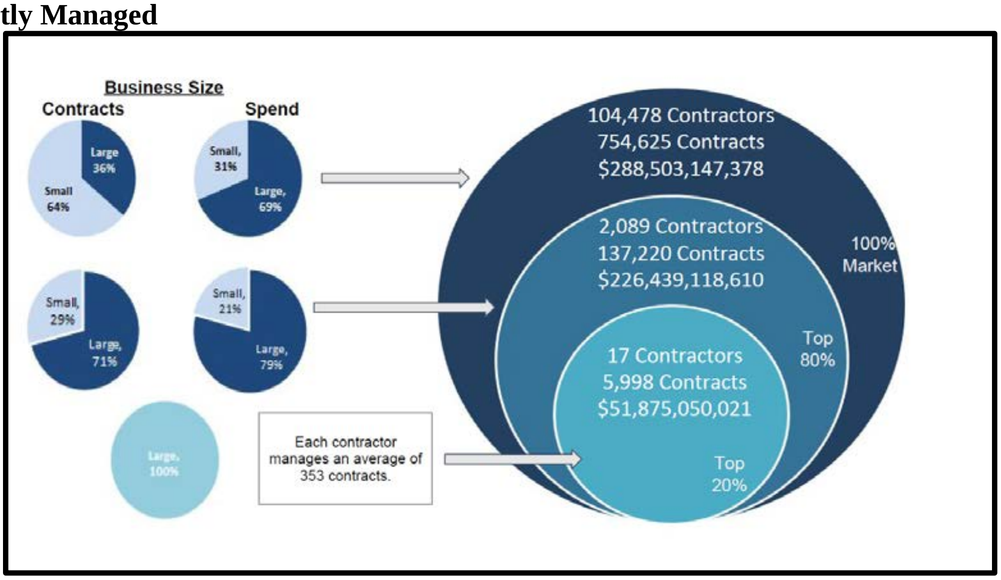
---

1. What do you see as GSA's best opportunity to streamline federal acquisition?

As part of the Agency Reform Plan that was recently sent to the Office of Management and Budget, GSA is exploring ways to streamline and reduce duplication in the GSA Schedules program and offer agencies expertise, improved supplier relationship management and modernized etools and purchasing platforms. Although it may ultimately require a multi-year process, streamlining and consolidating Schedules could offer significant end-to-end benefits to federal agencies, industry, and the taxpayer.

As illustrated below, there is a tremendous opportunity to significantly reduce contract duplication across government, which will result in substantial savings to agencies, industry and ultimately the American taxpayer.

FY 2016 10 Government-wide Spend Categories - Industrial Base by Spend and Contracts Currently Managed



2. How does GSA ensure the federal acquisition process reflects commercial best practices including reasonable pricing in acquisition vehicles, such as GSA schedule contracting?

The Multiple Award Schedules process for awarding a contract follows the Federal Acquisition Regulations (FAR) for “best value”. The factors considered in the process of identifying the best value for commercial products includes: warranty, delivery, price, and volume. MAS CO’s are required to stay current with their education and certification of their warrants and training includes updates and best practices as experienced across the program and made to regulation. It is the goal of FAS to provide GSA Contracting Officers and customer agencies with the latest and most accurate pricing intelligence to ensure procurements are made in the best interest of the Federal Government.

3. How many Federal Acquisition Regulation (FAR) and General Services Acquisition Regulation (GSAR) clauses apply for the acquisition of commercial goods and services? Please provide a list with title and cite for the clause.

While the actual number varies depending on requirements, up to 120 FAR and 70 GSAR clauses and provisions could apply to the acquisition of commercial items. Attached is a spreadsheet with FAR and GSAR Clauses/Provisions applicable to the acquisition of commercial items on the Multiple Award Schedule (MAS) (see attached document: FINAL MAS FAR and GSAR Clauses/Provisions Applicable to the Acq. of Commercial Items (tab 1) and FAR and GSAR- MAS clauses and provisions (tab 2)).

4. How will you use GSA's membership on the FAR Council to assess the current FAR and reduce the regulatory/compliance costs for federal contractors?

In accordance with Executive Order 13777, GSA’s regulatory reform task force is in the process of reviewing the regulations issued by GSA, including the GSA Acquisition Regulations, to identify opportunities to streamline acquisition and eliminate compliance costs for federal contractors. GSA solicited public comment through the Federal Register on May 30, 2017 for acquisition regulations reform ideas. As a member of the FAR Council, GSA will share the regulatory reform ideas with the other members of the FAR Council.

5. Currently, what services/tools does FAS provide to other agencies to assist with IT modernization and acquisition?

GSA provides a number of direct services, platforms and tools which assist Federal agencies in modernizing their IT and acquiring IT products and services.

For example, the Federal Acquisition Service (FAS) manages several large government-wide IT acquisition contracts through which agencies purchase more than $20 billion in IT products and services each year. IT Schedule 70 features more than 4700 highly qualified vendors, including Original Equipment Manufacturers (OEMs) and Value-added Resellers (VARs). Alliant, Alliant Small Business, VETS and 8(a) STARS are IT services government-wide acquisition contracts (GWACs) providing pools of highly qualified vendors, including small businesses. Additionally, GSA recently awarded the Enterprise Infrastructure Solutions (EIS) contract to replace the expiring Networx contract, ushering in the next generation of telecommunications and related products and services and providing these services to agencies at significant savings.

Also, the Technology Transformation Services (TTS/18F), built in the spirit of tech startups, acts as a consultancy for government, enabling agencies to rapidly deploy tools and services to create services for the public. Along with inter-governmental consultant services, TTS’ Office of Products and Programs (OPP), provides platforms and products agencies can utilize to more rapidly deploy IT capabilities into their enterprise. One example is Cloud.gov, a product built and maintained by TTS that provides mature cloud hosting services to agencies.

Additionally, GSA's Office of Governmentwide Policy (OGP) works directly with the Office of Management and Budget (OMB) on the Data Center Optimization Initiative (DCOI). The DCOI directly supports the Federal Information Technology Acquisition Reform Act (FITARA) of 2014 and provides agencies with support as they modernize and optimize their Data Centers.

These are just a few examples of the robust portfolio of IT services that GSA can bring to bear to assist agencies in modernizing their IT portfolio.

6. On July 6, 2017, GSA settled a whistleblower case brought by former Commissioner of the Federal Acquisition Service (FAS). The following questions relate to this case.

a. In Acting Administrator Tim Horne's response to the Office of Special Counsel concerning allegations raised by a whistleblower that were later substantiated, Horne noted that he instructed GSA's Senior Procurement Executive to review the existing delegations of procurement authority to TTS and determine whether any should be rescinded based on the reorganization.

i. What is the current status?

As a part of the "Joining Forces" efforts GSA has examined multiple facets of integrating TTS into FAS, including a working group examining TTS acquisition activities. This working group is focused on the development, implementation and maturation of TTS acquisition internal controls through FY18 and beyond. GSA is taking a risk-based approach to procurement delegations under the direction of the Senior Procurement Executive which limits the number and type of procurement actions TTS can perform. FAS intends to leverage best practices as well as use enterprise-wide procurement processes, controls and systems in procurement as a baseline while allowing TTS to mature their procurement practices.

ii. Have any delegations been rescinded? If so, which ones?

No delegations have been rescinded, however GSA reissued a new delegation to TTS in accordance with the plan outlined above on October, 18, 2017.

b. The Inspector General investigation examined possible violation of the Anti--Deficiency Act that, ultimately, was determined an Economy Act violation. The IG reviewed allegations that l8F improperly managed Interagency Agreements by backdating agreements in violation of the Economy Act and found 101 of 18Fs 202 project agreements predated the execution of the an Interagency Agreement.

i. How can such a large volume of agreements inappropriately be backdated?

18F began work on several engagements prior to signatures being executed due to lapses in internal controls and the desire to deliver services to agencies who needed work done quickly. This issue was resolved through enhancing internal controls for teams beginning work for agencies. For example, 18F no longer begins work in advance of agreement signatures as a matter of both policy and practice per the controls mentioned in the response to question ii below.

ii. What controls has GSA implemented to catch this type of systemic failure in the future?

GSA has documented and implemented a series of financial and management internal controls around the acceptance of Inter-Agency Agreements preventing the backdating of agreements. Below are a few of the specific internal controls now employed:

1. The Office of the Chief Financial Officer (OCFO) is now inserted into the agreement acceptance process. The last signature in the acceptance process of the agreement is made by the GSA OCFO. Additionally, a review and validation of the period of performance is done and that time.
2. System controls have been added to ensure all projects are linked to an appropriate funding source and billable work occurs only during the specified period of performance.
3. Monthly reconciliation processes have been instituted to ensure charges are properly allocated within the agreement period of performance, and that funds are available for billing/accrual purposes.

c. Have you personally reviewed the Inspector General's Investigative report on the recent GSA whistleblower reprisal case, specifically as it relates to TTS funding issues? Are you aware of any Anti-deficiency Act violations?

Yes, I have reviewed the report. No, I am not aware of Anti-deficiency Act violations.

d. Acting Special Counsel Adam Miles stated in his July 5, 2017 letter to the President and Congress that the reorganization of TTS may address concerns raised by the whistleblower case, but that "without additional details on improved management controls, the realignment does not address [the whistleblower's] substantiated concerns about mismanagement."

i. What is FAS' specific plan for improving internal controls to ensure TTS has accurate revenue projections? What are the financial controls in place?

The Inspector General’s evaluation of 18F’s business operations was conducted from December 2015 through September 2016. Since then, TTS (18F’s parent organization) has developed a corrective action plan in response to the IG report issued in October 2016 that addressed a number of financial and operating controls. They issued TTS-wide policy documents outlining these controls and communicated the changes to all employees.

GSA has implemented significant changes in the management approach for 18F to improve the operations of individual business units and TTS as a whole. In addition, TTS has implemented all the IG recommendations. We implemented all seven recommendations from "Evaluation of 18F." [1] In addition, we implemented all six recommendations from "Evaluation of 18F's Information Technology Security Compliance,"[2] including additional internal controls around hiring, revenue reconciliation and risk mitigation.

The program is monitoring the pipeline of actual and potential work orders to ensure that expenses are managed and workforce is utilized. Additional resources are only added if there is assurance of future work and capacity needs. Orders, pipeline, utilization and expenses are all closely monitored on a weekly and monthly basis. This process is a basis for the current plan to achieve full cost recovery.

As part of responding to the IG recommendations, TTS established new technical and procedural controls, including those related to when to begin billable project work and identifying funding sources at the beginning of engagements. TTS Policy for GSA Information FITARA Review requires GSA-CIO review and approval for all internal TTS contracts or agreements, as well as review and approval for external TTS contracts or agreements that leverage GSA IT platforms, security or infrastructure and conforms to GSA Policy 2101.1 CIO GSA Enterprise Information Technology Management (ITM) Policy. GSA has also developed extensive documentation of the TTS revenue generation, accrual, and reconciliation processes.

ii. What is FAS' specific plan for improving internal controls to ensure TTS has sufficient and not inflated staffing levels?

Please see response directly above to 6(d)(i).

[1] JE17-001, Evaluation of 18F, issued 10/24/16.

[2] JE17-002, Evaluation of 18F's Information Technology Security Compliance, issued 2/21/17.

Question for The Honorable Alan Thomas
Commissioner
General Services Administration, Federal Acquisition Service

Questions for the Record from Rep. Gerald E. Connolly, Ranking Member Subcommittee on Government Operations
House Committee on Oversight and Government Reform

July 12, 2017, Hearing: "General Services Administration - Acquisition Oversight and Reform"

---

1. Are there currently any existing or pending government contracts between the government and the Trump Organization?

There are no active acquisition contracts with any entity associated with the Trump Organization above the micro-purchase threshold reported to Federal Procurement Data System (FPDS) in accordance with Federal Acquisition Regulation (FAR) Subpart 4.6 Contract Reporting.

2. Has the General Services Administration (GSA) taken any steps to protect against a conflict of interest that could arise from government contracts with businesses owned by the President of the United States, his family members, or his business partners? If so, please describe those steps.

GSA's responsibility is to ensure that the government receives the best value for the taxpayer and to ensure that all procurements adhere to the FAR and other relevant rules, regulations and statutes, including those that address conflict of interest.

3. Could the Acquisition Services Fund be used to purchase goods or services from a business in which President Trump has financial interests?

Every procurement action undertaken by GSA must be in compliance with the FAR and other relevant rules, regulations and statutes.

4. Has GSA delisted Kaspersky Labs from its approved vendor's list for information technology services and digital photographic equipment? Does this prevent agencies from using Kaspersky Labs' products or will they still be able to purchase these products through other means?

Kaspersky Lab (KL) was neither a Multiple Award Schedule (MAS) vendor, nor a contract holder, with the U.S. General Services Administration (GSA); therefore, there was never any contract or other agreement with KL for GSA to terminate. As you know, GSA recently became aware that KL products were available on the product lists of three MAS vendors -- A&T Marketing Inc., Federal Merchants Corp., and Bahfed Corp.; however, KL products were not included as part of A&T Marketing's 2015 or Federal Merchants' 2012 Schedule 70 contract awards, or Bahfed's 2013 Schedule 67 contract award. Again, the KL products were not added via required contract modification requests, but rather were improperly added via the Schedule Input Program (SIP), a proprietary software provided by GSA, that allows contractors to update commercial catalogs electronically on GSA Advantage!®.

On July 11, 2017, GSA directed all three vendors to remove KL products from their product lists, which all three vendors subsequently did. GSA is complying with the Binding Operational Directive, issued by the U.S. Department of Homeland Security on September 13, 2017, in regards to KL products.

5. If Kaspersky Labs has been delisted, will agencies that already use Kaspersky software be able to continue to use that software following GSA's action?

Currently, agencies' use of Kaspersky products is governed by DHS BOD 17-01, which has directed agencies to identify their use of Kaspersky products within 90 days and then begin to remove identified products from agencies systems.

6. If Kaspersky Labs has been delisted, is GSA continuing further actions against Kaspersky Labs?

GSA did not have a contractual relationship with Kaspersky Lab and no further action is planned by GSA.

7. Section 4 of Executive Order 13-360 in 2004 directed GSA to establish a Government Wide Acquisition Contract (GWAC) at the agency. The purpose was to help Federal agencies meet their 3% goal of contracting with Service Disabled Veteran Owned Small businesses. This became known as the Veterans Technology Services (VETS) GWAC, or the VETS GWAC. On February 2, 2007, the VETS GWAC was awarded to forty-three (43) SDVOSBs and administered by the GSA Heartland Region 6 in Kansas City, MO with a base period of five years, expiring on February 1, 2012. On February 2, 2012, the first and only five-year option period was then awarded to qualified contract holders i.e. those initial contract holders that 1.) produced adequate revenue and 2.) had not grown revenue to exceed the $27.5 million NAICS Code 541512 threshold . This contract expired with the end of the option period on February 1, 2017. On April 21, 2016, the GSA issued a solicitation for a replacement to the VETS GWAC contract, with a short name of VETS2 GWAC. Bids were submitted on June 18, 2016 and as of today, there have been no contracts awarded to replace the original contracts.

   When does GSA intend to execute the replacement contract? Why has the replacement contract been so delayed? What is the timeline for an expected award of the replacement contract? Since the option period ended February 1, 2017 and the replacement contract has not been put into place, does that mean that all FY2017 opportunities have been are lost? If so, what is the dollar figure for lost SDVOSB opportunities since GSA did not have a replacement contract in place between June 2016 and February 2017 and what is the dollar figure for lost opportunities in FY2018?

GSA regrets not awarding VETS 2 contracts before the VETS GWAC expired. However, by taking the time to obtain industry and customer input, GSA believes that it has developed an improved VETS GWAC that will provide increased access to SDVOSBs. GSA understands the importance of the VETS 2 GWAC to the Service-Disabled Veteran-Owned Small Business (SDVOSB) community and is expediting its evaluation of proposals. The Solicitation was issued on April 21, 2016 and closed on June 20, 2016. GSA received over 175 proposals to review and evaluate.

On August 22, 2017 GSA published the required pre-award notice for small business programs in FedBizOpps, announcing that evaluations were complete and listing the apparent successful offerors. On October 26, 2017, GSA announced the award of the VETS 2 contracts to 70 SDVOSB firms.

Lost business volume for the next fiscal year is projected to be very low as there are several alternative contract vehicles available including GSA Schedule 70, NASA SEWP and VA's T4 Next Generation

(T4NG) contract. In addition, agencies can conduct set aside acquisitions using Alliant Small Business and STARS 2 and GSA offers assistance to agencies in using alternative solutions. Obligated dollars through IT Schedule 70 to SDVOSBs over the previous fiscal years is $687.7M in FY 15, $740.3M in FY 16 and $795.3M in FY17.

8. FedRAMP has made significant progress over the past year and a half. Cloud service providers are more prepared to go through the Authorization to Operate (ATO) process and the ATO process timeline has been reduced from 18-24 months down to an average of four months. What steps does GSA plan to take to continue to improve the FEdRAMP program? How does stakeholder engagement fit into GSA's plans to improve FedRAMP?

First, GSA will continue to ensure that all JAB authorization decisions occur in less than 6 months so that no authorization effort will take longer than 6 months. This commitment to timeline was a direct output of the FedRAMP Accelerated initiative that began in FY16.

Second, GSA released a FedRAMP Tailored Baseline requirements for Low Impact Software as a Service. The requirements for this baseline are reduced from 126 down to 36 and has a reduced set of documentation requirements as well. It’s expected that authorizations under this process could happen in as quickly as 4-6 weeks. The Tailored Baseline requirements are designed for low risk cloud solutions that many digital service teams and agencies either currently use or have a need to use - tools that focus on collaboration, project management, and open source development and public engagement.

Similar to the redesign efforts that FedRAMP undertook to reduce the authorization timelines via FedRAMP Accelerated and FedRAMP Tailored, FedRAMP is doing the same thing for the ongoing efforts associated with Continuous Monitoring once systems get authorized. Although much attention is given to the initial assessment, the Continuous Monitoring by FedRAMP of Cloud Service Providers is significant, with monthly reviews of vulnerabilities and yearly assessments, as well as reviewing changes to systems after authorization. FedRAMP just finished the research phase of this effort by working with a broad range of vendors and agencies to understand capabilities and needs. The design and implementation phase is just getting underway and is expected to be completed by the end of FY18. FedRAMP believes that this effort can help reduce the level of effort for government and vendors by anywhere from 25%-50%.

GSA is also looking at ways to automate portions of FedRAMP - from process and business flow, to creating machine-readable formats for all of the templates and so that agencies can use whatever tools they have in place currently to help them automate the authorization process. This includes partnering with industry tool vendors on how to best promote interoperability, with over 40 respondents to a recent request for information.

The voice of the customer and stakeholder engagement is at the heart of all of the major initiatives that FedRAMP undertakes. FedRAMP completes post authorization surveys with every vendor, and has regular check-ins with vendors on how FedRAMP can improve. GSA also releases an annual survey where, in the most recent version, 82% of respondents had a favorable rating of the program, and all major changes to the policy or requirements go through two rounds of public comment before being finalized to ensure we hear from all stakeholders on the impact and feasibility of any changes.

9. What is GSA doing to help agencies improve their FITARA Scorecard performance on data

center consolidation?

GSA's Data Center Optimization Initiative Program Management Office (PMO) serves as a resource to help agencies implement DCOI optimization plans by facilitating participation in interagency data center shared services; sharing best practices and information about tools for improving data center efficiency; and supporting agencies reporting on progress toward FITARA goals. The Data Center PMO mission and goals reflect its role in carrying out DCOI policy by establishing a customer-centric approach to empowering agencies to meet optimization and efficiency goals. The Data Center PMO's mission is to define, design, implement, and monitor a set of government-wide IT infrastructure solutions which leverage data center community input.

10. How is GSA currently evaluating any supply chain concerns, including foreign ownership and influence, or foreign investment, in contractors seeking to get onto federal government contract vehicles?

GSA has implemented numerous supply chain risk management strategies and GSA continues to further explore additional opportunities, particularly through interagency groups and partnerships with other agencies. Some specific examples of GSA efforts include:

- Contractors are required to make representations and certifications through FAR Clause 52.212-3 when completing the award process on GSA contract vehicles. Through this clause contractors represent whether they are a foreign entity, whether they are an inverted domestic corporation, the place of manufacturer, compliance with Trade Agreements Act and Buy American Act as applicable. GSA Contracting Officers rely on these representations and certifications in making responsibility determinations prior to award of contract.

- During contract administration, GSA engages in a number of supply chain risk management activities such as utilizing data analytics to identify product authenticity and utilizes Industrial Operational Analysts to review contractor compliance with requirements such as providing Trade Agreement Act compliant products through the Multiple Award Schedules (MAS) program. When GSA Contracting Officers are informed through data, Industrial Operations Analysts or other sources on potential non-compliance they take appropriate contract action to address compliance with contractual requirements.

Question for The Honorable Alan Thomas
Commissioner
General Services Administration, Federal Acquisition Service

Questions for the Record from Rep. Stephen F. Lynch Subcommittee on Government Operations
House Committee on Oversight and Government Reform

July 12, 2017, Hearing: "General Services Administration - Acquisition Oversight and Reform"

---

1. A provision of the National Defense Authorization Act for fiscal year 2018 would require the Administrator of GSA to establish a program for the procurement of commercial goods through online marketplaces.

One section of the online marketplace provision states that the award of a contract to the marketplace provider or providers -the entities establishing the online purchasing sites - "may be made without the use of full and open competition."

Full and open competition, with certain limited exemptions, has been the gold standard in federal procurement since passage of the Competition in Contracting Act in 1984.

Competition helps to ensure that the government receives the best value for the American taxpayer.

a. If this provision were to become law, would GSA use full and open competition to award the online marketplace provider contracts? If not, how would you ensure that taxpayers receive the best value?

Competition is a guiding principle in our procurement system as stated in the Federal Acquisition Regulation. GSA intends to use competition in the selection of platform providers, unless an enumerated statutory exception to competition is justified. Based on its current understanding of the market, GSA believes competition it is the ideal avenue to achieve best value for the Government and the taxpayer and does not envision a specific scenario where an exception would be invoked.

2. The federal government has invested considerable resources into existing online ordering programs, like the Federal Supply Schedules and Defense Department's FedMall. The online marketplace provision established by the NDAA would seem to be in direct competition with those existing programs. Please answer the following :

a. What impact do you think the provision would have on the existing programs?

GSA is looking at opportunities to streamline access to the federal market for vendors and simplify procurement for agencies, mirroring how taxpayers purchase in the commercial world. As a part of this implementation, GSA would implement a commercial platform in a considered and phased roll-out.

GSA intends to implement the enacted provision (section 846 of the FY 18 NDAA), in concert with ongoing initiatives, to ensure the best use of taxpayer dollars and efficient technology tools.

b. The NDAA proposal would allow for decentralized purchasing. How would this align with current federal purchasing programs like Strategic Sourcing and Category Management?

The Section 846 language aligns well with the fundamental principles of strategic sourcing and category management. In particular, section 846 anticipates that platforms which are part of the program would capture data on the purchases to provide visibility into those purchases and allow agencies to evaluate and compare results (e.g., pricing, small business participation, other considerations) from different acquisition strategies, including decentralized purchasing vs. coordinated purchases through category management. This discretion is reinforced by section 846(b), which makes clear that use of the authority is discretionary and not intended to displace other authorities (which would include buying strategies) whose use would be more appropriate. and Section 846(c)(2)(C), which requires GSA and OMB to conduct an assessment of the products or product categories that are suitable for purchase on the commercial e-commerce portals as part of the phase II report that is due to Congress in March 2019.

c. How does GSA propose to reconcile the NDAA's proposed language, which would prohibit modification of the online marketplace's terms and conditions, with the existing unique government requirements for purchasing?

GSA is meeting with key stakeholders regarding the implementation of NDAA section 846 including vendors of e-commerce platforms, industry providers to the federal government, customer agencies as well as the oversight community to determine the best way forward. The first listening session was held on January 9, 2018. GSA is now reconciling comments from that feedback session. In particular, GSA recognizes that there are some differences between online marketplace terms and conditions and existing government requirements. Through ongoing active agency and industry outreach, GSA will gain a deep understanding of government agency requirements and of portal providers' terms and conditions. This knowledge will help inform the phase II report, due to Congress in March 2019.

Questions for The Honorable Rob Cook
Deputy Commissioner (Director, Technology Transformation Services)
Federal Acquisition Service

Questions for the Record from Chairman Will Hurd Subcommittee on Information Technology
House Committee on Oversight and Government Reform

July 12, 2017, Hearing: "General Services Administration -Acquisition Oversight and Reform"

---

1. In August 2016, a GAO report (GA0-16-602) made two recommendations to GSA related to 18F. Has 18F implemented GAO's recommendations?

   TTS has developed outcome oriented program goals and associated performance measures for 18F to include cost recovery metrics. The FAS Commissioner, the Chief Financial Officer and the TTS Director review 18F performance measures and cost recovery on a regular basis.

   a. If not, when do you expect to implement these recommendations? N/A

2. What percentage of 18F employees have been hired via Schedule A authority?

   Currently, 89% of 18F staff were hired via the Schedule A Authority.

3. Do you see 18F continuing to grow in size or staying where it is now?

   18F began FY 2017 with a staff of 169, and has decreased in size during the year, finishing FY 2017 with a staff of 123. During FY 2018, we are planning steady staffing of approximately 150. 18F has adjusted its management approach to ensure that staff size correlates to demand and is working closely with the GSA CFO to ensure that growth does not outpace business volume.

   a. Will the percentage of Schedule A positions increase, decrease, or stay the same?

   We continue to seek the best mix of Schedule A and competitively hired permanent employees to attain the strongest mix of technical skills to continue helping the federal government modernize its information technology.

4. When do you project 18F will achieve full cost recoverability?

   In response to the corrective action plan issued as a result of the Inspector General reports, TTS is moving as quickly as possible in the direction of full cost recovery and expects to achieve full cost recovery in fiscal year 2019For instance, in conjunction with FAS leadership, 18F is making operational adjustments, such as increasing staff utilization rates, to achieve cost recovery.

5. Are there controls in place to measure and ensure that the work 18F is performing is targeted to recover its costs?

   Yes. 18F takes cost recovery seriously. We have made operational improvements and developed controls to manage financial success. 18F analyzes its cost recovery and sales pipeline weekly. TTS, 18F's home organization, works closely with the CFO's office to reconcile billing monthly and conducts monthly financial reviews with the CFO and TTS leadership.

6. The Federal Risk and Authorization Management Program (FEDRAMP) is a GSA led government-wide program to certify the cybersecurity of cloud products and services. This Committee would like to ensure that administrative hurdles to widespread adoption of cloud solutions are minimal and security of such solutions is sufficient. Certain stakeholders and media reports have indicated that the GSA's FedRAMP process takes too long and is too costly. [1]

   a. What is the average time it takes a cloud services provider to clear the FedRAMP process?

   The FedRAMP Program Management Office at GSA has worked over the last 18 months to drastically reduce the time it takes to achieve an authorization through the Joint Authorization Board. Through that work the timing was reduced by 75% to approximately 12-16 weeks for an Authority to Operate (ATO) decision, down from an average of 18 months.

   b. Typically, what are the causes of delays in obtaining FEDRAMP certification?

   The typical causes for a delay center around the vendor not having all the correct technical security controls fully implemented, in particular: multi-factor authentication, Federal Information Processing Standard (FIPS) and NIST validated encryption, and configuration management and vulnerability management (e.g. resolving vulnerabilities in a timely manner). Industry reports that FIPS assessments, which are mandated by law (e.g., not FedRAMP program) can often take upwards of 16-24 months.

   To help clarify these expectations, FedRAMP released a rapid FedRAMP Readiness process for vendors to work with industry auditors and third party assessors to ensure that they have all of the key technical pieces in place before beginning a FedRAMP assessment. To date, over 30 vendors have actively participated in this readiness process as they build out their service to ensure they have the key technical pieces in place to achieve a FedRAMP authorization.

c. How much does it cost for a cloud service provider to go through the FEDRAMP process? Please provide the high and low range of such costs and any information indicating how these costs have changed over time.

One company (Coalfire Federal) recently completed research[3] around the costs associated with obtaining a FedRAMP authorization and found them to be between $350,000 and $865,000 depending on a cloud provider's readiness, overall complexity, and pre-assessment activities. Clearly, large vendors providing government-wide platforms can require more investment, but we're continuing to drive this cost down by redesigning processes and leveraging the potential for automation.

The Coalfire study found that the costs associated with achieving a FedRAMP authorization was comparable to other compliance regimes such as Service Organization Control (SOC) II, Payment Card Industry Data Security Standard (PCI DSS), and International Standards Organization (ISO) 270001.

d. How many agencies currently use FEDRAMP certified products and services?

There are over 120 agencies working with FedRAMP - this includes agencies in all three branches of government - Executive, Judicial, and Legislative

e. How can the FEDRAMP process be improved?

We're continually looking for ways to improve the process, and some of our most recent work has been partnering with industry to identify ways to streamline the continuous monitoring aspect of FedRAMP. Most people consider the upfront assessment, and don't realize that we conduct monthly reviews with each provider to ensure they maintain high levels of security standards, such as patching high-security vulnerabilities within 30 days. This means that the government makes a long-term commitment in promoting the security of critical internet-based companies, often benefiting commercial institutions that leverage these same providers. As a small organization, we continue to re-evaluate how we allocate costs and work with our industry partners to streamline the security review and oversight processes.

Additionally, GSA released a FedRAMP Tailored Baseline requirements for Low Impact Software as a Service. The requirements for this baseline are reduced from 126 down to 36 and has a reduced set of documentation requirements as well. It's expected that authorizations under this process could happen in as quickly as 4-6 weeks. The Tailored Baseline requirements are designed for low risk cloud solutions that many digital service teams and agencies either currently use or have a need to use - tools that focus on

[3] https://www.coalfire.com/The-Coalfire-Blog/May-2017/Meeting-FedRAMP-Standards-Report

collaboration, project management, and open source development and public engagement.

f. Are there potential improvements that may be realized through legislation?

We believe that improvements to the security processes that secure and safeguard our Federal infrastructure are strongly tied to IT modernization activities. We appreciate the committee's oversight of this subject, and we believe continued dialogue around the topic is critical. For FedRAMP specifically, it's largely a voluntary requirement for agencies, and a recent study by Deltek- plus positive media impressions[4] showed that vendors continue to recognize the value of FedRAMP certification and the improvements to the program. Continued legislative attention on IT modernization and security, in partnership with other key Federal stakeholders, can help the program increase value over time.

7. On May 17, 2017, the House passed the Modernizing Government Technology Act (H.R. 2227). This legislation is designed to incentivize federal agencies and CIOs to transition from legacy systems to modern, more secure systems, including cloud solutions. The bill also assigns a significant role to GSA related to the centralized Technology Modernization Fund.

   a. What expertise will GSA bring to fulfill the MGT Act objective of modernizing federal government IT?

GSA will bring a range of expertise and resources to help achieve the goals of the Act. For example, within the Federal Acquisition Service, TTS has in-house technical and product experts, who can help ensure that investments through the Technology Modernization Fund are focused on delivery. Within FAS more broadly, GSA has significant procurement expertise to help ensure that agencies receive the best-in-class from industry and service providers. Finally, as a centralized shared-service provider within the federal government, GSA is uniquely positioned to offer shared services and platforms to enable agencies to reduce the number of duplicative legacy systems.

   b. What work is GSA and specifically TTS currently doing to modernize federal IT government-wide? Please provide a sampling of such projects and cost savings realized.

TTS has a number of mature offerings within the Office of Products and Programs (OPP), such as FedRAMP, api.data.gov, the Digital Analytics Program, and the USAGov Contact Center, that collectively save an estimated $100 million annually. Additionally, 18F has saved agencies millions of dollars through its consulting work and its main production product offering, cloud.gov. For example, the Federal Election Commission has reported that

[4] Positive press samples: https://goo.gl/s29U4D, https://goo.gl/DkvQit, https://goo.gl/wp6HmC

it will be able to reinvest $1.2 million annually by using cloud.gov. Finally, through authorities granted by the Intergovernmental Cooperation Act, the TTS Office of Acquisition has helped multiple federal and state agencies modernize legacy systems, with substantial cost avoidance and savings, and faster delivery cycles.

8. The Committee is concerned that the Government may be developing products that compete with the private sector, and waste government resources when a commercial alternative is available.

   a. For example, why did 18F build cloud.gov?

   Current infrastructure and platform solutions available to government do not have built-in compliance and security measures that address federal guidelines. As 18F was building IT solutions for agencies, we did not have a way to quickly access infrastructure without building costly and time consuming custom solutions on top of it. We saw a deep need for modern infrastructure that would reduce the time to delivery, especially reducing the effort associated with developing solutions within government regulations and security considerations.

   b. Does cloud.gov compete with private sector providers?

   c. When cloud.gov first launched, GSA's intent was to assist federal agencies in delivering citizen-facing services in a faster, more user-centered way. As GSA has worked with its industry partners and customers to better understand cloud hosting needs, the cloud.gov model has matured and evolved to better recognize the changes and advancements made by the private sector in this space. It remains GSA's intent that, to the greatest extent possible, cloud.gov should not compete with private sector providers when solutions that adequately address government-specific needs are available. To help ensure this, it is GSA's plan moving forward to use cloud.gov as a way to deploy prototypes and create appropriate templates and standards for open source federal hosting, similar to a sandbox. GSA will work closely with its customers, when ready for full production, to source and procure the appropriate cloud hosting environment from among commercially available options. What procedures are in place to ensure GSA is selecting commercially available IT solutions (Buy vs Make) in compliance with the Clinger Cohen Act, FITARA and OMB Al30 reporting?

   GSA firmly believes that government should build solutions only when a private sector solution is unable to meet government demands. In carrying out that principle, GSA ensures all IT acquisitions are in compliance with federal policies, regulations and statutes. There are controls in place at GSA to ensure IT acquisitions follow long-established acquisition procedures. All IT purchases for systems operated by GSA are reviewed and approved by the GSA CIO as required by FITARA and OMB policy. The cloud.gov platform, in particular, is underpinned by a variety of products and services purchased from the commercial marketplace. For instance, TTS currently purchases AWS infrastructure from a Service-Disabled Veteran-Owned Small Business (SDVOSB) reseller and the platform uses many other private sector Software-as-a-Service tools, such as PagerDuty.

9. In your testimony, you mentioned 18F's role in assisting Treasury with implementing the DATA Act, but didn't mention 18F's role helping OMB implement the DATA Act's procurement pilot for recipient reporting.

   a. Please describe 18F's past/current role in the procurement pilot?

   The 18F team focused on prototyping potential solutions for reducing contractor burden and evaluating their viability through user research and testing. The learnings generated by prototyping were presented to GSA’s Office of Governmentwide Policy to inform the development of a production model that may be piloted.

   b. Who was primarily responsible for implementing the procurement pilot?

   The Office of Management and Budget’s Office of Federal Procurement Policy (OFPP) was responsible for the strategic direction and management of the pilot with GSA managing the design, development, and delivery of the technology solution.

   c. When was GSA first approached to work with OMB on the pilot?

   18F was first approached in March 2015.

   d. How many contractors participate in the pilot?

   One contractor, NuAxis, built the pilot system.

   e. The procurement pilot focuses on Davis-Bacon reporting (on payment of prevailing wages. How was Davis-Bacon reporting selected? Why made this decision?

   The initial reporting requirement for the tool is the method by which contractors certify their proper payment of prevailing wages as required by the Department of Labor’s regulations implementing the Davis-Bacon Act (See 29 CFR 3.3, 5.5(a)(3)). The recently released OMB report on the pilot outlines in detail how OMB selected these areas. The idea was to prototype a tool to simplify the reporting process to enable contractors to remain in compliance with these regulations while reducing reporting burden.

10. The Committee understands 18F may have done projects for state governments. The Committee is concerned that this effort and associated resources could be better spent addressing IT challenges within the federal government.

   a. Please describe the work 18F may be doing for state governments, by project, cost and dates.

18F is working with state governments via the authority provided in the Intergovernmental Cooperation Act (IGCA). Like many federal agencies, state and local governments face enormous IT challenges and every year receive billions of dollars in federal grant funds to modernize and improve their IT systems.

When work is linked to federal projectsfunding, the 18F Acquisition team collaborates with both federal and state/local partners to help states responsibly spend federal grant money by providing acquisition and technical consulting for improving state IT systems. Active projects are:

- **State of California**
  - Medicare and Medicaid enrollment and eligibility (not to exceed $350,000 through 6/30/2018)
  - Child welfare systems (not to exceed $575,000.00 through 6/30/2018)
- **State of Alaska**:
  - Medicare and Medicaid enrollment and eligibility (not to exceed $1,770,000 through 6/30/2018)
  - Child welfare systems (not to exceed $300,000 through 6/30/18)
- **State of Vermont**
  - Medicare and Medicaid enrollment and eligibility (not to exceed $1,000,000 through 6/30/2018)

b. Does 18F plan to continue work for state and/or local governments?

When linked to federal projects/funding, 18F will work with state and local governments in order to help states responsibly spend federal grant money dedicated to IT modernization. We will only undertake those projects on a fully-reimbursable basis and in compliance with all applicable statutes and regulations.

GENERAL SERVICES ADMINISTRATION
QUESTIONS FOR THE RECORD RESPONSES
FOR
HOUSE OVERSIGHT AND GOVERNMENT REFORM SUBCOMMITTEE ON
TRANSPORTATION AND PUBLIC ASSETS
"FEDERAL MANAGEMENT: OVERSIGHT OF LEASED VEHICLES" HEARING
HELD
FEBRUARY 26, 2016

1. To what extent, if any, is the disposal or sale of federal vehicles centralized through GSA rather than handled by individual agencies?

Answer 1 (GSA-only): GSA Fleet disposes of all vehicles that it leases to its customer agencies in a centralized manner. GSA Fleet vehicles do not typically go through the disposal process and are instead sold under the exchange-sale authority so that the proceeds of sale can be applied to replacement vehicles. GSA Fleet only leases approximately one-third of the Federal fleet to agencies. The remaining two-thirds of the Federal fleet consist of agency-owned vehicles. Agencies that own their own vehicles must utilize GSA's Personal Property program or dispose of the vehicles themselves.

Answer 1 (Government-wide): Executive agencies are required to select an Office of Management and Budget (OMB) approved Federal Asset Sales center to sell their surplus personal property unless they receive a waiver from the GSA Office of Government-wide Policy to sell property through other means (FMR 102-38.40). GSA's Personal Property Sales Program is one of seven approved sales centers and is the only sales center that sells all commodity types, nationwide. Many civilian agencies utilize GSA's Personal Property Sales Program to sell their vehicles. GSA however does not generally sell vehicles owned by the Department of Defense (DoD) and the Department of Homeland Security (DHS). Both these agencies are approved sales centers whose authority includes sale of vehicles.

The GSA Personal Property Sales Program disposes of motor vehicles in the same manner as any other type of property. Before selling a vehicle, GSA screens the property for potential use by other Federal agencies and eligible donees. Vehicles that survive utilization and donation screening are competitively auctioned to the general public via the GSAAuctions.gov website. All sales on GSAAuctions.gov are also simultaneously posted to the Government-wide sales portal, GovSales.gov.

2. What is the average mileage of vehicles sold from the federal fleet? GSA testified there are minimum, pre-sale mileage levels established by regulation, but that norms vary by agency and by vehicle use as well as condition. Does GSA maintain data on mileage at point of sale?

Answer 2 (GSA-only): Yes, GSA maintains data on mileage at point of sale. The average miles for the GSA Fleet leased vehicles that sold from fiscal year 2013 through 2015 was

51,653, 52,366, and 53,097 miles, respectively. The average premium GSA Fleet vehicles sold for above the Fair Market Value as measured by Blackbook was 114%, 115%, and 111%, respectively, for the same fiscal years.

The minimum replacement criteria for all Federal Government vehicles are set forth in the Federal Management Regulation at section 102-34.270. All agencies, including GSA, must adhere to these minimum requirements when replacing vehicles.

GSA Fleet has established minimum replacement criteria for the portion it owns and leases to agencies at a higher level (higher age and miles) than the minimum prescribed in the Federal Management Regulation. These are minimum replacement standards and are set taking into account all acquisition and operational costs including maintenance and repair costs, timing of manufacturer warranties, and vehicle sale proceeds. Maximizing the sales proceeds from the disposal of vehicles plays an important role in GSA Fleet's operation as it does not receive annual appropriated funds. The proceeds are used to procure new vehicles. Newer, more fuel efficient vehicles cost less to operate and maintain and provide a reliable vehicle that agencies can count rely on as they perform their mission.

GSA Fleet's minimum replacement criteria are set to maximize the return for the Government while ensuring customer agencies have safe, reliable vehicles they need to meet their mission requirements and are reviewed and refined at least annually to ensure optimal replacement standards. GSA Fleet continues to monitor its minimum replacement criteria to ensure it maximizes the return for the Government and its customers have the vehicles they need to meet their mission requirements.

Answer 2. (Government-wide): The average mileage of vehicle sold through GSA's Personal Property Sales Program in fiscal years 2014 and 2015, was 84,446, 82,384 and 85,418 miles for passenger vehicles, light trucks, and other vehicular equipment, respectively. Passenger vehicles include sedans and station wagons. Light trucks consists of minivans, pick-ups, SUVs (4X2 and 4X4s) and light duty trucks. Other vehicular equipment consists of ambulances, buses, medium and heavy duty trucks and specialized equipment. These figures do not include seized/forfeited vehicles sold by GSA that were not used in Federal service and these figures do not include GSA Fleet leased vehicles.

When customer agencies report vehicles to GSA's Personal Property Sales Program for disposition, a current odometer reading is required and captured in GSA's systems. Since the reporting agency maintains custody of the vehicle throughout the disposal process, only they can attest to veracity of the odometer reading reported. GSA believes that the odometer readings reported by agencies are generally accurate with occasional outliers.

3. What requirements exist for public notification prior to a federal vehicle sale or auction?

Answer 3 (GSA-only): GSA Fleet leases approximately one-third of the Federal fleet to agencies. The remaining two-thirds of the Federal fleet consist of agency-owned vehicles and therefore GSA Fleet can only provide responses that contain information on the one-third of the fleet that it leases. The Government is required to provide access to the general public for all vehicle auctions. GSA Fleet posts information about vehicle auctions on Facebook, Twitter, and the GSA Fleet AutoAuctions website (https://autoauctions.gsa.gov/GSAAutoAuctions/). Additionally, the vendors are contractually required to advertise all GSA Fleet vehicle sales. The vendors typically use print and radio, along with television and other independently determined methods. The AutoAuctions website and the vendors' advertising are the basic means the general public learns of vehicles being sold.

Answer 3. (Government-wide): The Executive agency conducting the sale generally must first publicly advertise for bids in a manner that permits full and free competition (FMR 102-38.55).

Vehicles sold by the GSA Personal Property Sales Program are advertised and auctioned to the general public on GSAAuctions.gov. Vehicles are also simultaneously posted to the Government-wide sales portal GovSales.gov for additional exposure. GSA also advertises, at times, through print media, internet, and social media to generate public awareness of GSAAuctions.gov and property available for sale.

4. What are the average mileage and sale price paid for used federal vehicle sold from federal inventory? If possible, provide these data by vehicle type.

Answer 4 (GSA-only): GSA Fleet leases approximately one-third of the Federal fleet to agencies. The remaining two-thirds of the Federal fleet consist of agency-owned vehicles and therefore GSA Fleet can only provide responses that contain information on the one-third of the fleet that it leases. For GSA Fleet vehicles:

Vehicle Type	FY 2013		FY 2014		FY 2015	
	Average Miles	Average $	Average Miles	Average $	Average Miles	Average $
Passenger	44,687	$9,205	44,726	$9,134	47,306	$8,679
Light Duty	54,872	$10,160	56,269	$11,108	56,229	$12,267
Other	70,852	$11,334	69,975	$12,630	70,097	$12,746

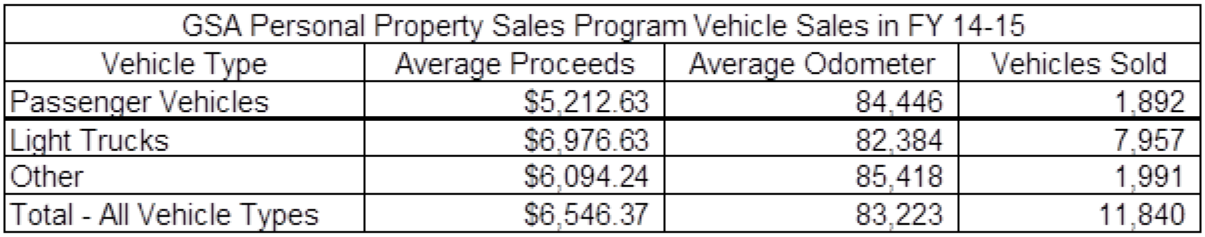
Notes:

- Passenger vehicles includes sedans and station wagons

- Light Duty vehicle includes minivans, 4X2 and 4x4 pickup trucks and 4x2 and 4x4 sports utility vehicles
- Other category includes ambulances, buses, medium and heavy duty trucks, and non-motorized vehicles (e.g., trailers)

Answer 4. (Government-wide): The average mileage of vehicle sold by GSA's Personal Property Sales Program in fiscal years 2014 and 2015, was 84,446, 82,384 and 85,418 for passenger vehicles, light trucks, and other vehicular equipment, respectively.

The average selling price of vehicle sold by GSA's Personal Property Sales Program in fiscal years 2014 and 2015, was $5,212.63, $6,796.63 and $6,094.24 for passenger vehicles, light trucks, and other vehicular equipment, respectively.



GSA Personal Property Sales Program Vehicle Sales in FY 14-15			
Vehicle Type	Average Proceeds	Average Odometer	Vehicles Sold
Passenger Vehicles	$5,212.63	84,446	1,892
Light Trucks	$6,976.63	82,384	7,957
Other	$6,094.24	85,418	1,991
Total - All Vehicle Types	$6,546.37	83,223	11,840

Passenger vehicles includes sedans and station wagons. Light trucks consists of minivans, pick-ups, SUVs (4X2 and 4X4s) and light duty trucks. Other vehicular equipment consists of ambulances, buses, medium and heavy duty trucks and specialized equipment. These figures do not include seized/forfeited vehicles sold by GSA that were not used in federal service and these figures do not include GSA Fleet leased vehicles.

5. Has Amtrak submitted data to GSA's FAST system?

Answer 5: For purposes of Federal motor vehicle reporting, Amtrak is not a department, agency, or instrumentality of the United States Government. Rather, Amtrak is operated and managed as a for-profit corporation. The Department of Transportation does not report AMTRAK Fleet data to the FAST system.

6. Please provide copies of the types of reports GSA issues to agencies to assist them in fuel card management and reduction of related abuse. If the reports vary in detail, please provide the most detailed versions available.

Answer 6: GSA Fleet helps customers appropriately address vehicles with usage statistics significantly outside of the norm through a comprehensive online tool (Fleet Drive-thru), which provides the customer with on-demand detailed vehicle-specific data, including gallons of fuel consumed, details around alternative fuel usage, and total miles driven. The fuel use reports can be customized to provide data about the agency as a whole or to provide detailed transactional data at the individual vehicle level. Total miles driven and average monthly miles driven reports for the fiscal year are designed to allow the customer to make robust forecasting decisions. The attached document “GSA Fleet Drive-thru Report Fields” provides an overview of all the data available to customers’ on-demand in GSA Fleet Drive-thru.

7. Please provide any explanatory text, notes, or guidance that would normally accompany the National Account Report.

Answer 7: The National Account Reports are developed by GSA Fleet and shared at the headquarter level of most of GSA Fleet's customer agencies by their respective GSA Fleet National Account Advisory Team (NAAT). Each GSA representative will discuss the contents of the report and further assess customer agency needs during their annual customer briefing. The report serves as a standard outline designed to foster constructive dialogue between GSA and its customers around the major areas impacting the customer’s vehicle fleet.

The report is organized in the following manner:

- Current Vehicle Inventory and Utilization
- Vehicle Acquisition Stats
- Optional Equipment Rate Charges
- Fuel Use and Miles Reporting
- Accidents and Incidents
- Agency Incurred Expense
- Short Term Rental Expense
- Projected Vehicle Replacements

While the report has a set layout, each GSA NAAT has a specific insight/knowledge/intelligence of their particular customer agency. He or she typically highlights key areas of the report with the aim of addressing specific customer priorities that might lead to more effective and efficient management their fleet vehicles.

8. Please describe GSA’s short term rental program for vehicles and equipment.

Answer 8: GSA Fleet’s Short Term Rental (STR) program supplies vehicles and equipment to all federal agencies to fulfill short term and temporary needs. The program offers a wide selection of vehicles and equipment to meet seasonal work, special events, disaster response and surge requirements. STR is also a valuable solution to replace vehicles/equipment temporarily out-of-service for repairs and maintenance. Vehicles can be rented for up to 120 days, and equipment for up to 365 days.

The STR program is a cost-effective resource that saves agencies time and money. GSA takes care of all procurement requirements to provide customers with quick access to vehicles and equipment at the lowest available rates. With the STR program, GSA handles all the contracting requirements so customers focus on their mission and not duplicate acquisition effort.

Benefits of the STR program include:

- Lowest available commercial rates
- Easy, hassle-free procurement
- Convenient online request system, available 24/7
- Fuel cards provided
- Tax-exempt rentals (in most states)
- Charges conveniently appear as a line item on your GSA Fleet invoice
- No fee for additional drivers

Since its launch in 2007, STR demonstrates continued growth. Over 80,000 vehicles have been rented, with over 12,000 rentals occurring in fiscal year 2015.
http://www.gsa.gov/str

9. Please provide information on how and by what specific date GSA will have implemented the GAO recommendations related to the vehicle management issued in its 2016 report titled *Federally Leased Vehicles: Agencies Should Strengthen Assessment Processes to Reduce Underutilized Vehicles* (GAO-16-136).

Answer 9: GSA received three specific recommendations laid out in the final GAO report, *Agencies Should Strengthen Assessment Processes to Reduce Underutilized Vehicles (GAO-16-136).* Recommendations are as follows:

- To help improve the accuracy of Drive-thru data to allow agencies to better manage their leased vehicle fleet data, we recommend that the Administrator of GSA evaluate the 9,999-mile/month electronic safeguard for Drive-thru odometer readings to determine if a lower threshold could improve the accuracy of customer data and adjust it accordingly.
- To provide better assurance that Fleet Service Representatives (FSRs) are having conversations with the leasing customers about utilization in accordance with GSA expectations, we recommend that the Administrator of GSA develop a mechanism to help ensure that these conversations occur.
- To help strengthen the leased vehicle justification processes across federal agencies, we recommend that the Administrator of GSA examine the [Federal Property Management Regulation] FPMR to determine if the regulations should be amended to require that vehicle justifications are clearly documented and readily available, and adjust them accordingly.

GSA has developed subsequent actions to implement each of the recommendations, respectively.

- GSA Fleet will evaluate the 9,999-mile/month electronic safeguard for Drive-thru odometer readings in an effort to optimize data integrity, balanced with the ease of use and administrative workload of GSA Fleet and its customers.
- GSA will evaluate existing protocols to ensure that Fleet Service Representatives (FSRs) are having conversations with leasing customers about utilization in accordance with GSA Fleet management expectations.

- GSA will review the FPMR to determine if existing regulations should be amended to strengthen the leased-vehicle justification processes across federal agencies. This review is underway and comprehensive of the entire regulations.

Each of these actions will be completed by the end of calendar year 2016 (12/31/2016).

10. What policies do you have in place to inform employees of their rights as whistle blowers?

Answer 10: The following policies are in place to inform GSA employees of their rights as whistle blowers:
1. Employees' rights to Whistleblower Protection located at http://www.gsa.gov/portal/content/101978.
2. Merit System Principles and Prohibited Personnel Practices located at https://www.gsa.gov/portal/content/101978.
3. *1025.3 ADM P Protecting Whistleblowers with Access to Classified Information*. This policy provides agency direction and guidance on Protecting Whistleblowers with Access to Classified Information. The policy ensures employees serving in the Intelligence Community or those who are eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information. Additional information may be found at: https://insite.gsa.gov/portal/content/656510.

11. How often do you require your employees to complete training on whistleblower protections?

Answer 11:

· GSA annually provides mandatory training on the No FEAR Act for all GSA employees. This course covers the rights and remedies available to Federal employees under both anti-discrimination laws and whistleblower protection laws. New employees and new managers/supervisors must take the No FEAR Act training within 90 days of being hired.

· GSA provides mandatory supervisory training on Merit System Principles and Prohibited Personnel Practices. This course provides employees with the knowledge and skills needed to uphold the merit system principles and avoid prohibited personnel practices to include reprisal for whistleblowing. The training is mandatory for all new supervisors upon commencement of being appointed to a supervisory position; and then every three years thereafter.

· GSA partnered with the Office of Special Counsel who provided Whistleblower Protection Act training to GSA supervisors and managers. The training provided an explanation of the rights of federal government employees who whistleblow on government wrongdoing. The training was provided last year.

· All new GSA employees are orientated during New Employee Orientation on the merit system principles, prohibited personnel practices, and the whistleblower protection act. New Employee Orientation is conducted on a bi-weekly basis.

12. What is the punishment in your agency for retaliating against a whistleblower?

Answer 12: The Agency reviews potential disciplinary actions on a case-by-case basis in accordance with the GSA Penalty Guide for offenses, which ranges from a warning notice to removal.

13. Is your agency in compliance with the Whistleblower Protection Enhancement Act's standards for non-disclosure agreements?

Answer 13: Yes.

14. How many employees at your agency are currently on administrative leave as a result of an ongoing investigation?

Answer 14: There are currently 2 GSA employees on administrative leave pending investigations for misconduct.

14a. In the past year, how many employees at your agency have been placed on administrative leave as a result of an ongoing investigation?

Answer 14a: In the past year, a total of 9 GSA employees were placed on administrative leave. Of the 9, 2 cases are open and 7 cases are closed.

14b. How long was/is each individual on administrative leave?

Answer 14b: Of the two open cases, one employee has been on administrative leave for 68 days and the other employee has been on administrative leave for 153 days.

With regard to the 7 closed cases, the number of days was as follows: 1) 9 days; 2) 188 days; 3) 181 days; 4) 113 days; 5) 276 days; 6) 75 days; and 7) 56 days.

15. What operating system does the Agency use?

Answer 15: GSA uses several different operating systems including Windows, Unix, Mac OS and Linux.

16. How much does the Agency spend annually on maintaining IT systems?

Answer 16: Total O&M Without Other agency funding
FY15 O&M 465.33M

FY16 O&M 473.89M
FY17 O&M 476.85M

17. How often do you meet with your CIO and your chief information security officer?

Answer 17: The GSA Fleet Automated Solutions Division meets with its OCIO counterparts on a daily basis. The meetings are a combination of regular Change Control Board (CCB) sessions to track the status of ongoing initiatives and coordinate appropriate action, and ad hoc meetings to address specific issues. In addition, the managing leads of the Automated Solutions Division and their OCIO counterparts meet monthly to coordinate and address concerns (to include systems security) at a higher level.

The CIO Division Director and Branch Chief responsible for support of GSA Fleet automated systems meet both monthly and on an ad hoc basis with the Information Systems Security Manager (ISSM) to discuss and address security matters directly related to these systems. Further, all newly developed systems are security scanned prior to implementation and continue to be scanned on a weekly basis for life of the system. Any findings are reported to the OCIO's Information System Security Officer (ISSO) for remediation. Service tickets are opened to track all actions through completion of remediation.

18. Have you had a penetration test done on your network in the last year?

Answer 18: Yes, GSA conducts annual agency network penetration tests.

18a. IF YES, Do you know how long the white hat hackers were in the Agency's network before they were discovered?

Answer 18a: N/A - The testers did not breach the system/network.

19. The President issued a memorandum in 2009 directing agencies to adopt a presumption of openness. Has your agency adopted a presumption of openness?

Answer 19: Yes.

19a. If so, how has that changed FOIA operations at your agency?

Answer 19a: GSA restructured its FOIA Operations to a centralized structure to increase agency-wide accountability to FOIA laws and regulations and ensure that the FOIA program is operating with a presumption of openness. Under a centralized structure, the GSA subject matter expert (SME) performs the initial review and determination about the records and the appropriate disposition. Once the SME has made a determination, he or she consults with a FOIA professional. The SME and FOIA professional must reach an agreement regarding the release before the determination and records are forwarded to the GSA Office of General Counsel (OGC). OGC reviews the documents and determination. OGC must provide approval and concurrence prior to the GSA FOIA Program Manager approving release to the requester. In the absence of a compelling reason, GSA will disclose a record even if it otherwise is subject to exemption (41 C.F.R. 105-60.103-2).

19b. Can you provide some examples of records that have been released since your agency adopted this presumption of openness that you would not have otherwise released?

Answer 19b: GSA releases records and material that may otherwise have been covered by the fifth statutory exemptions under FOIA, 5 U.S.C. § 552(b)(5). Examples of information released include records containing information regarding the agency's deliberative process. The releases are made after conducting an analysis for foreseeable harm, per the guidance provided by the DOJ - Office of Information Policy and the memoranda issued by the President and the Attorney General. Example of these releases include memorandum of internal agency policies and procedures, including accompanying emails regarding the functioning of GSA programs. Programs highlighted in these discretionary releases include internal process and procedure information releases on GSA's Travel and Charge Card, Fleet Management, Federal Building Leasing, general acquisition, and Property Disposal programs.

20. How does your agency apply the presumption of openness to the deliberative process privilege when responding to FOIA requests? How does the agency determine that records need to be withheld under deliberative process privilege?

Answer 20: GSA views all FOIA release decisions through a prism of openness. GSA's approach is predisposed towards disclosure in the review and release of documents. The agency's policies require discretionary disclosures whenever possible and provide that:

> "GSA will not withhold a record unless there is a compelling reason to do so; i.e., disclosure will likely cause harm to Governmental or private interest. In the absence of a compelling reason, GSA will disclose a record even if it otherwise is subject to exemption." (41 C.F.R. 105-60.103-2)

Multiple steps ensure that the presumption of openness is being applied to all decisions involving FOIA at GSA. GSA program offices are responsible for searching for, locating, and reviewing the responsive records. Once the records are located, GSA FOIA professionals collaborate with the GSA program office subject matter experts (SMEs) to examine the documents and make an initial determination whether there is a compelling reason to withhold information. GSA program office managers perform a secondary assessment of the records being withheld, the proposed redactions and justifications for withholding any parts of the records. Any proposed redaction or withholding of any part of the records requires concurrence from the responsible GSA program officials and the Office of General Counsel prior to release to the requester. If there is no compelling reason to withhold information, the record is released.

21. How much training did your FOIA staff receive in the past year?

Answer 21: All of the GSA FOIA professionals attended multiple substantive formal FOIA training sessions during the past year. Each GSA FOIA professional attended a variety of FOIA courses, receiving a minimum of six hours of official formal FOIA training. Courses included:

- Freedom of Information and Privacy Act training offered by the Graduate School USA;
- FOIA training provided at the American Society of Access Professionals 2015 National Conference;
- “The Freedom of Information Act for Attorneys and Access Professionals” offered by Department of Justice;
- Best Practices Workshops offered by the Department of Justice
    - “Best Practices from the Requester’s Perspective”
    - “Implementing Technology to Improve FOIA Processing”
    - “Customer Service and Dispute Resolution”.

22. How much training does agency-wide staff receive on FOIA and federal record responsibilities?

Answer 22: The vast majority of program office Subject Matter Experts (SMEs) that assist on GSA FOIA request processing attended a substantive FOIA training during the past year. The GSA Freedom of Information Act (FOIA) Requester Service Center conducted several types of FOIA training for GSA employees whose roles and responsibilities involve the FOIA. The GSA FOIA Requester Service Center made several Regional site visits nationwide to conduct in-person FOIA training, as well as attending many GSA office and program staff meetings at GSA Central Office in order to provide FOIA training. The GSA FOIA Requester Service Center also held webinar training sessions throughout the year for all key segments of GSA employees that are involved in GSA Freedom of Information requests.

GSA has undertaken several communication and outreach methods to inform non-FOIA professionals of their obligations under the FOIA. GSA employees are continually made aware that FOIA is every employee’s responsibility. GSA FOIA professionals engage GSA’s non-FOIA professionals through a variety of outreach meetings and training sessions, as well as presenting at assigned Directors and GSA Office and Division staff meetings. During these times, FOIA professionals are able to reiterate the importance of FOIA responsibilities as well as provide necessary training and updates. Additionally, the GSA Chief FOIA Officer sends out memorandums with updates and key information regarding FOIA processes and responsibilities in a continual effort to ensure accountability of the FOIA program at GSA.

Also, during the past year, the GSA FOIA professionals revised and reissued the agency-wide GSA FOIA Handbook and Desk guide, as well as developed and issued an internal FOIA Service Level Expectation (SLE) document. These reference documents cover the responsibilities and required actions and services provided by agency FOIA SMEs and the GSA FOIA Requester Service Center to successfully administer the FOIA regulations and provide GSA FOIA requesters excellent customer service and timely responses to FOIA requests.

All GSA employees are required to take a yearly records management policy and procedures course. This course is found on the GSA Online University and reviews current and new policies and procedures that must be followed. It covers all aspects of records management, from the records inventory process through records disposition.

23. What is your progress on DATA Act implementation?

Answer 23: Working with the Office of the Chief Financial Officer, GSA IT and the Office of Governmentwide Policy, have developed a data-driven approach to implementing the requirements of the DATA Act, using the draft guidance provided to date by

OMB/Treasury. GSA is awaiting final guidance from OMB/Treasury DATA Act PMO, which is expected at the end of April.

24. Have you fully mapped the data required by Treasury and OMB?

Answer 24: GSA has fully mapped the draft versions of the data requirements and is awaiting final guidance in April from OMB/Treasury.

25. Do you expect to be fully compliant by May 2017?

Answer 25: Provided that GSA obtains final guidance on the data elements and reporting architecture in April, the agency is expected to be fully compliant by May 2017.

26. How does the agency plan to use the data being produced through this DATA Act effort to improve efficiency and decision-making?

Answer 26: As the agency builds out its solution to support the DATA Act, GSA will leverage the tools and information to provide insights about its and customer agencies' spending on acquisitions.

27. How much has the agency spent on DATA Act implementation? Why?

Answer 27: To date, the Agency has obligated $598,013.06 for contract technical assistance, to help develop the data environments to bring together data from multiple systems, and build the reporting architecture.

28. In the last 5 years, have there been any violations or allegations of violations of the Federal Records Act? If so, what were they?

Answer 28: In the last 5 years, there have been two allegations of violations of the Federal Records Act related to the improper deleting of records. In both cases, the individuals involved deleted electronic records prior to their disposition date and did not save them into a system of record. However, in both cases the email records were retrievable and saved accordingly. The persons involved have been retrained on how to address, maintain and save records according to NARA's General Records Schedule (GRS) and GSA's Records Retention Schedule.

29. Do you still use a "print-to-file" records retention system?

Answer 29: Yes.

29a. If yes, are you planning to transition to an electronic system? When?

Answer 29a: GSA still utilizes a “print-to-file” records retention system, but GSA is transitioning to an electronic document management system (EDMS) that meets NARA’s requirements for an electronic recordkeeping system. The implementation of this system will begin in the second quarter of FY16 and is projected to be completed in FY18 prior to the December 2019 mandated deadline.

For email records, GSA is using Google Vault and NARA’s Capstone approach to meet the Presidential and OMB mandate to save email in an electronic system of record. GSA’s proposal for a capstone approach implementation strategy has been submitted to NARA for approval. Once approved, GSA will begin implementation immediately and expects to be completed prior to the mandated December 2016 deadline.

29b. If no, when did you change?
Answer 29b: Please see answer 29a. above.

30. When did you last update your agency's Federal Records Act guidance regulations and policy?

Answer 30: In FY15, GSA’s Records Retention Schedule was updated to include NARA’s latest guidance. GSA’s records management guidance regulations and policy are scheduled to be updated in FY16.

GSA

Office of Congressional and Intergovernmental Affairs

August 19, 2016

The Honorable Will Hurd
Chairman
Subcommittee on Information Technology
Committee on Oversight and Government Reform
House of Representatives
Washington, DC 20515

The Honorable Mark Meadows
Chairman
Subcommittee on Government Operations
Committee on Oversight and Government Reform
House of Representatives
Washington, DC 20515

Dear Chairman Hurd and Chairman Meadows:

Thank you for your letter dated August 3, 2016, requesting responses from the U.S. General Services Administration (GSA) Technology Transformation Service (TTS) to your Questions for the Record from the joint June 10, 2016, hearing titled, "18F and U.S. Digital Services Oversight." Acting Commissioner David Shive requested that I respond to your inquiry.

Enclosed are GSA's detailed responses to your questions regarding 18F's services, security, and the Acquisition Services Fund, as well as supporting materials included in Appendix 1. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

Lisa A. Austin

Lisa A. Austin
Associate Administrator

cc: The Honorable Robin L. Kelly, Ranking Member, Subcommittee on Information Technology
The Honorable Gerald E. Connolly, Ranking Member, Subcommittee on Government Operations

Enclosures (2)

Questions for Mr. David Shive
Acting Commissioner, Technology Transformation
Service General Services Administration

Questions from Chairman Will Hurd
June 10, 2016, Hearing:
"18F and U S. Digital Service Oversight"

---

1. **Please provide a list and a description of each project 18F has worked on, in any capacity, that is related to the Office of Management and Budget's list of top ten highest priority IT investment projects. For each project please include details of the services provided, when 18F services began, and indicate when 18F's services were completed or, if they are ongoing, the anticipated date of completion.**

- **Census 2020**
    - Census Digital Transformation
        - Status: Ongoing
        - Period of Performance: 10/7/2015-9/25/2016
        - Details of Service: 18F has provided technical expertise, mentorship, and code enhancements to the Census team working on Primus, which is the Census-built version of the citizen-facing component of the 2020 Internet data collection application.

- **Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) Transformation**
    - MyUSCIS
        - Status: Completed
        - Period of Performance: 5/1/2015-4/30/2016
        - Details of Service: MyUSCIS helps users more easily navigate the immigration process. 18F helped to reimagine and modernize immigration and visa processes by building tools that improve the applicant process, providing clear and simple information to the public, and creating new tools that make the processing of immigration forms faster and more efficient.
    - USCIS Identity, Credentialing, and Access Management (ICAM) Development
        - Status: Completed
        - Period of Performance: 7/8/2014-5/1/2015
        - Details of Service: USCIS Public ICAM is a login and identity-verification system for people wanting to interact with

USCIS. Built with industry-standard tools and using modern practices, it uses USCIS and the State Department's own information to verify immigrants' identities. Currently and primarily serving immigrants renewing their Green Cards, the system has over half a million users. 18F was called in to partner with USCIS on the development of the system to ensure the timely launch the project, allowing hundreds of thousands of immigrants the ability to renew their Green Card online.

- USCIS Infrastructure as a Service (three total IAAs for this project)
    - Status: Completed
    - Period of Performance: 5/1/2015-6/12/16
    - Details of Service: Provided access to, and consolidated billing for, infrastructure services, platform services, and software services and other tools that may be labeled generally as being part of "cloud services."

- **Department of Veterans Affairs (VA) Veterans Benefits Management System (VBMS)**
  - Veterans Affairs VBMS Software Development Kit
    - Status: Completed
    - Period of Performance: 7/22/2015-7/20/2016
    - Details of Service: VA engaged 18F to build one or more Ruby "gems" to interface with the existing VBMS Application Programming Interface (APIs). Ruby is a computer programming language. A Ruby gem is a self-contained Ruby program that can be easily reused and redistributed. The requested gem provides a single point of communication with the three VBMS services in order to streamline the development process of creating applications that process veterans' benefits claims. Such applications retrieve and store documents related to specific disability claims, and perform other related business processes related to claims, such as moving a claim to appeals.

- **Social Security Administration, Disability Case Processing System (DCPS)**
  - Disability Case Processing System Agile Acquisition Consulting
    - Status: Completed
    - Period of Performance: 10/27/2014-9/30/2015
    - Details of Service: 18F provided agile coaching and acquisition consulting services to support the DCPS program's transition from waterfall to agile practices. We conducted agile training sessions, delivered an assessment of the overall program and provided recommendations for maturing program and product delivery, and produced an

agile solicitation in alignment with those recommendations.

2. **The Department of Veterans Affairs accounts for 3 of the top 10. Please provide a list and a description of each project 18F has worked on at the Department of Veterans Affairs. For each project please include details of the services provided, when 18F services began, and indicate when 18F's services were completed or, if they are ongoing, the anticipated date of completion.**

    - Veterans Affairs VBMS Software Development Kit
        - Status: Completed
        - Period of Performance: 7/22/2015-7/20/2016
        - Details of Service: VA is engaging 18F to build one or more Ruby "gems" to interface with the existing VBMS Application Programming Interface (APIs). Ruby is a computer programming language. A Ruby gem is a self-contained Ruby program that can be easily reused and redistributed. The requested gem provides a single point of communication with the three VBMS services in order to streamline the development process of creating applications that process veterans' benefits claims. Such applications retrieve and store documents related to specific disability claims, and perform other business processes related to claims, such as moving a claim to appeals.

    - Veterans Affairs Cloud Migration
        - Status: Ongoing
        - Period of Performance: 8/31/15-8/30/16
        - Details of Service: 18F provides Infrastructure as a Service (IaaS) cloud computing and engineering support for the creation and launch of Veterans.gov. 18F provided the procurement vehicle to allow VA to migrate to a commercially provided IaaS vendor.

3. **Please provide a list and a description of each project 18F has worked on at the Census Bureau. For each project please include details of the services provided, when 18F services began, and indicate when 18F's services were completed or, if they are ongoing, the anticipated date of completion.**

    - Census Digital Transformation
        - Status: Ongoing
        - Period of Performance: 10/7/2015-9/25/2016
        - Details of Service: 18F has provided technical expertise, mentorship, and code enhancements to the Census team

working on Primus, which is the Census-built version of the citizen-facing component of the 2020 Internet data collection application.

4. **Does 18F envision its role as being an entity that fixes single, identifiable IT problems at an agency or helping agency IT personnel learn how to manage and fix their IT problems themselves?**

Over the last two and a half years, 18F has grown from a small team focused on building prototypes and web services to an organization with five business units:

- **Custom Partner Solutions.** Provides agencies with custom application solutions.
- **Products and Platforms.** Provides agencies with access to tools that address common Government-wide needs.
- **Transformation Services.** Aims to improve how agencies acquire and manage IT by providing them with consulting services, to include new management models, modern software development practices, and hiring processes.
- **Acquisition Services.** Provides acquisition services and solutions to support digital service delivery, including access to vendors specializing in agile software development, and consultations on developing requests for proposals.
- **Learn.** Provides agencies with education, workshops, outreach, and communication tools on developing and managing digital services.

18F's ultimate goal is to transform the way the government builds, buys, and shares digital services. We accomplish this mission by providing teams of digital services experts (designers, engineers, researchers, product specialists) using modern methodologies (agile software development, developer operations practices, user-centered design) to help agency customers rethink the way they deliver services online.

Our end goal of transformation ensures that the focus isn't solely on creating or buying software, but rather delivering a solution in partnership with an agency that meets the needs of the user first and leaves that transformation capability behind at the agency. It is imperative that we work hand-in-hand with our customer agencies so that we ensure modern methods are learned by our customers, not simply bought. We will continue to adapt to our customers' needs, and look forward to a future where all agencies work in the manner that delivers the best quality results for the public: in the open, putting users first throughout the development cycle, and iteratively in short cycles to minimize risk.

5. **Why did 18F choose to build cloud.gov, a Platform as a Service (PaaS)**

rather than pursuing an existing, open source, commercially available PaaS solution?

Cloud.gov does use an existing, open source, and commercially available PaaS solution. 18F customized a mature open source PaaS, called Cloud Foundry, and is deploying it on our commercial Infrastructure as a Service (IaaS) provider, in this case, Amazon Web Services.

As 18F matured, we found that we needed a PaaS that would serve the extensive compliance requirements of Federal teams. We took the Cloud Foundry project and built onto it to fit the specific needs of Federal technology development and procurement.

The core goal of cloud.gov is to radically reduce the time and labor it takes for Federal teams to gain Authority To Operate (ATO) for applications. Cloud.gov is an open-source project that other commercial providers can borrow from and reuse.

a. **Is the cloud.gov service FedRamp compliant?**

Cloud.gov is going through the FedRAMP compliance evaluation process. We received "FedRAMP Ready" status in May 2016, and we hope to receive FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) in November 2016.

6. **Ms. Chrousos testified that 18F has one service line that builds prototypes and light web services, but this service does not compete with the private sector. Rather the service is a means to showcase modern methodologies and practices to agencies. What process does 18F follow in order to determine when 18F should build a service and when the service should be purchased from a private sector service provider?**

18F is committed to delivering solutions that best meet the needs of our agency customers' user base. The first step in evaluating a partner's needs is a thorough exploration of the challenges facing the agency and their users. This period of "discovery" generally entails getting to know the end users, better understanding stakeholder needs, and honing in on what problem we can help solve. Often times it is clear from the outset that our acquisitions unit will help the agency rethink what is needed in a procurement, and help draft a modern, modular-based procurement request. Sometimes, the result of this discovery process determines the need for custom software. When this is the case, the evaluation team first considers any low-cost buy options, then considers the reuse of open-source code. If these options do not exist, the team considers the creation of custom software. As Federal employees ourselves, we recognize the value in not creating custom software for challenges easily solved with a commercially available option.

7. **The Federal Information Security Management Act (FISMA) requires agencies to assess the effectiveness of their information security controls and OMB Circular A-130 requires that agencies assess and authorize their systems before placing such systems in an operating environment. This end result of this process is typically for an IT system to receive an Authority to Operate (ATO). Does 18F have current ATOs in place for its IT systems? What is the process for 18F ATOs?**

   18F does not currently have ATOs for all of their systems. There are known shortcomings in the coordination of the ATO process between GSA IT and 18F, and we are working next steps to resolve any gaps. GSA IT and 18F are currently coordinating so that 18F is following the overarching agency guidance, GSA IT Security Procedural Guide 06-30[1], to receive ATOs. Additionally, TTS is appointing an infrastructure lead that will manage the technical strategy for the organization, in accordance with GSA technology policies. This includes coordinating ATOs with the Office of the Chief Information Security Officer within GSA IT.

8. **When l8F acquires free open source software, what process or security protocols/updates are implemented to ensure the software is secure?**

   When 18F acquires external software for use in processing agency data or production data, it is subject to security review by 18F and GSA IT during the Authority to Operate process, whether open source or proprietary in nature. While the software 18F produces itself is almost entirely open source, 18F acquires a mix of free open-source software and proprietary software to accomplish its mission. Because software being open source does not carry any inherent security risks in comparison to proprietary software, it is treated identically during security reviews.

   a. **Does l8F consider costs of modifying the free open source to ensure it is compliant with all applicable security standards?**

      Yes, 18F does consider costs of modifying the free open source to ensure it is compliant with all applicable security standards.

   b. **If l8F does calculate these costs, does 18F then compare the**

[1] GSA IT Security Procedural Guide 06-30 is included as an appendix to our response. Please note that this guide is an internal GSA document and is for OFFICIAL USE ONLY. This Guide cannot be shared, published, or distributed on the internet or to people that do not have a need to know.

modification costs to the costs of commercially available products or services that are compliant, out of the box, with applicable security standards?

18F considers the cost of any modification or configuration it may need to perform when acquiring software in order to meet Federal security standards or GSA/18F policies, whether proprietary or open source. Open source software is not inherently less compliant with Federal security standards than proprietary software.

9. **Products in use by the Federal Government must be compliant with federal security standards. What is the process 18F follows to ensure the products developed by 18F are compliant with these security standards?**

18F is working with GSA IT to follow GSA IT Security Procedural Guide 06-30, which is included as an appendix to this response, in order to better assess systems in accordance with Federal security standards, as well as receive approval from the Chief Information Security Officer and 18F's Executive Director, prior to release.

18F, like all organizations in GSA, is expected to adhere to Federal and GSA IT security requirements.

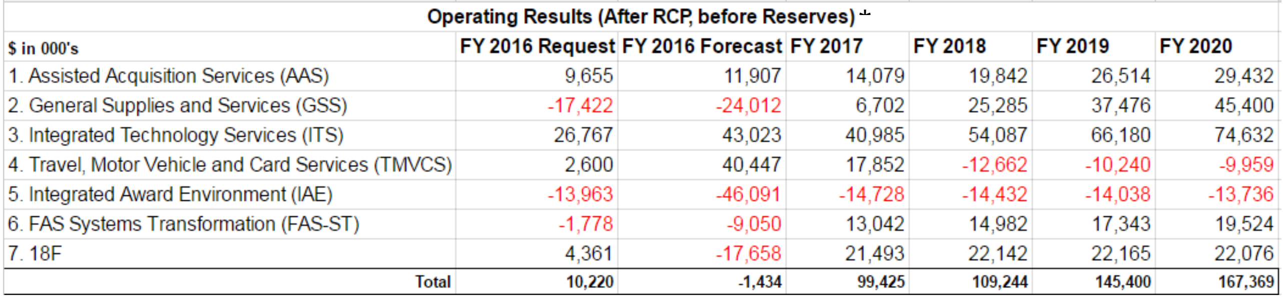
a. **Has 18F ever requested waivers to any Federal security standards?**

18F requested a waiver for sub-domains related to the Domain Name System Security Extensions (DNSSEC) security requirement. GSA IT granted this waiver request.

10. **At the hearing, Congressman Walker requested a list of GSA's business units that generate revenue for GSA's Acquisition Services Fund. Please provide a list of these business units, along with each individual unit's projected revenues or deficits by year for the next five years**.

The Acquisition Services Fund (ASF) is organized around four major business portfolios and three initiatives that deliver solutions to partner agencies. The projections below align to the revenue projections for fiscal year (FY) 2017 presented in the FY 2017 GSA Congressional Justification, which is formulated 18 months prior to release. The out-year estimates include the same assumptions used for the FY 2017 revenue projections.

GSA is in the process of formulating the FY 2018 Congressional Justification, which will include revised numbers for FY 2016, FY 2017, and FY 2018 from those that are projected in the table below. We anticipate a variance from plan in FY 2017. ASF projected total operating results after replacement cost pricing (RCP), before reserves, that is between 1-2 percent of total revenue. We are happy to share those updated numbers when they are finalized and released in the FY 2018 Congressional Justification.



Operating Results (After RCP, before Reserves) *

$ in 000's	FY 2016 Request	FY 2016 Forecast	FY 2017	FY 2018	FY 2019	FY 2020
1. Assisted Acquisition Services (AAS)	9,655	11,907	14,079	19,842	26,514	29,432
2. General Supplies and Services (GSS)	-17,422	-24,012	6,702	25,285	37,476	45,400
3. Integrated Technology Services (ITS)	26,767	43,023	40,985	54,087	66,180	74,632
4. Travel, Motor Vehicle and Card Services (TMVCS)	2,600	40,447	17,852	-12,662	-10,240	-9,959
5. Integrated Award Environment (IAE)	-13,963	-46,091	-14,728	-14,432	-14,038	-13,736
6. FAS Systems Transformation (FAS-ST)	-1,778	-9,050	13,042	14,982	17,343	19,524
7. 18F	4,361	-17,658	21,493	22,142	22,165	22,076
Total	**10,220**	**-1,434**	**99,425**	**109,244**	**145,400**	**167,369**

*The ASF is authorized to retain earnings to cover the cost of replacing fleet vehicles (RCP).This table includes operating results after taking RCP into consideration. The ASF is also authorized to retain earnings for funding certain anticipated operating needs, also known as reserves, specified by the Cost and Capital Plan. Please note- the table below does not show reserves amounts

APPENDIX 1:

GSA IT Security Procedural Guide 06-30: Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment

Office of the Chief Information Security Officer

IT Security Procedural Guide: Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA) CIO-IT Security-06-30

Revision 9

May 19, 2016

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 Changes – March 22, 2006				
1	Bo Berlas	Included the OWASP Web Application Penetration Checklist and the OWASP Testing Project documents as embedded objects into Appendix C – GSA Risk Assessment Security Requirements.	To provide a usable checklist for testing the OWASP Top Ten Vulnerabilities.	14
Revision 2 Changes – February 13, 2007				
1	Bo Berlas	Various updates to reflect changes in A&A process	FINAL publishing of NIST 800-53 on 12/2006	4-10
2	Bo Berlas	Updated Appendix A: Risk Assessment Report Format	RA and SA are now combined into a single RA/SA report.	11
3	Bo Berlas	Updated Appendix B: GSA Security Assessment Test Procedures	Updated Assessment test procedures based on FINAL publishing of NIST 800-53 on 12/2006	15
4	Bo Berlas	Updated Appendix C: Plan of Action and Milestone (POA&M) Template	Attached new POA&M template for FY 2007.	16
5	Bo Berlas	Updated Appendix D: Risk Assessment / Security Assessment Plan Template	Updated assessment plan template to reflect combining of RA and SA reports.	17
Revision 3 Changes – March 20, 2007				
1	Bo Berlas	Changed reference to OWASP Top Ten from 2007 Release Candidate 1 back to the 2004 Update.	OWASP Top Ten, 2007 RC1 has not been finalized. GSA will adopt the OWASP Top Ten, 2007 Update upon final publication.	6
2	Bo Berlas	New database scanning requirement.	App Detective or similar tool should be used to test database security configurations.	7
Revision 4 Changes – October 16, 2007				
1	Bo Berlas	Updated policy reference.	GSA IT Security Policy was updated June 2007.	6
2	Bo Berlas	Changed reference to OWASP Top Ten from the 2004 Update to the current 2007 Update.	The 2007 Top Ten lists current web application vulnerabilities.	7

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
3	Bo Berlas	Replaced the FY 2007 POA&M Reporting Template with the FY 2008 template.	New OMB Quarterly POA&M Reporting Requirements	17
Revision 5 Changes – July 15, 2010				
1	Bo Berlas	Update the A&A process to be consistent with NIST 300-37 and the Risk Management Framework	Updates required to ensure agency compliance.	Various
2	Bo Berlas	Inserted Roles and Responsibilities relating to A&A from the GSA IT Security Policy	Identify A&A Roles and Responsibilities	3
3	Bo Berlas	New implementation guidance for NIST 800-53 controls.	To facilitate implementation of required controls	25
4	Bo Berlas	New NIST 800-53 assessment test cases	Required to facilitate assessment of NIST 800-53 controls	Appendix C
5	Bo Berlas	New OCISO A&A Review SOP	Documents the process for submission of A&A packages to the OCISO and the detailed procedural steps performed by the OCISO to verify A&A compliance.	Appendix E
6	Bo Berlas	New guidance for A&A of Minor Systems	To facilitate assessment of minor systems.	22
Revision 6 Changes – December 16, 2010				
1	Bo Berlas	Updated references for Certification, Accreditation, and Certification and Accreditation (C&A) to Assessment, Authorization, and Assessment and Authorization (A&A), respectively.	To be consistent with the current terminology in NIST 800-37.	Throughout
2	Bo Berlas	Inserted guidance for forming sections 1-10 of the SSP for cloud computing system SSPs.	To address cloud specific security challenges.	12
Revision 7 Changes – May 31, 2011				
1	Bo Berlas	Updated references to A&A to security authorization process and authorization package or A&A package to security authorization package.	To be consistent with the current terminology in NIST 800-37.	Throughout

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
2	Bo Berlas	Inserted guidance for review of minimal impact SaaS solutions.	To document required review activities for such systems.	25
3	Bo Berlas	Updated Appendix E to include a revised OCISO Security Authorization Package Review SOP.	To reflect current version of the SOP.	48
Revision 8 Changes – November 25, 2015				
1	Lewis/ Sitcharing	Changes made throughout the document to reflect NIST and GSA requirements	Updated to reflect and implement the most current NIST 800-53-Rev4 and GSA requirements	Various
Revision 9 Changes – May 19, 2016				
1	Wilson/ Klemens	Restructuring of the document, modifications to specific process descriptions.	Updated to reflect current acceptance of risk process and rename Minor Application process to Subsystem process and revise its description. Restructuring and editing throughout.	Various

Approval

IT Security Procedural Guide: Managing Enterprise Risk, Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA), CIO-IT Security-06-30, Revision 9 is hereby approved for distribution.

X

Kurt Garbars
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

1 Introduction

The General Services Administration (GSA) agency-wide Security Assessment and Authorization (A&A) Process is based on the National Institute of Standards and Technology (NIST) Risk Management Framework and the security authorization process as described in the latest NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.

This guide describes key activities in managing enterprise-level risk through a system life cycle perspective including system security authorization and continuous monitoring. It is designed to assist agency and contractor personnel with security responsibilities in implementing the process.

1.1 Purpose

This procedural guide defines the GSA risk management process, specifically the security authorization process GSA has implemented for information systems to obtain a full authorization to operate (ATO). The guide describes the key activities in managing enterprise-level risk as described in NIST SP 800-37.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal Employees, contractors and associates of GSA who oversee/protect GSA information systems and data. The guide provides GSA associates and contractors as identified in the GSA Order CIO 2100.1, Information Technology (IT) Security Policy, and other IT personnel involved in performing A&A activities, the specific processes to follow for properly accomplishing A&A activities for the systems under their purview.

1.3 Policy

As detailed within CIO 2100.1, Authorizing Officials (AO) must ensure risk assessments are performed as part of A&A activities before a system is placed into production, when significant changes are made to the system and at least every three (3) years unless it is covered by GSA's Continuous Monitoring (ConMon) Program.

1.4 Assessment and Authorization Roles and Responsibilities

There are many roles associated with the security authorization process. System Owners for each information system are responsible for ensuring their respective Service/Staff Office (S/SO) systems have been through the GSA security authorization process, have received an ATO from the AO, and received concurrence from the GSA Office of the Chief Information Security Officer (OCISO). The complete roles and responsibilities for agency management officials and others with significant IT Security responsibilities are defined fully in CIO 2100.1. The following sections provide a high level description of the responsibility for the primary roles with management and operational A&A responsibilities.

1.4.1 GSA Administrator

The GSA Administrator is responsible for ensuring an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of GSA.

1.4.2 GSA Chief Information Officer (CIO)

The GSA Chief Information Officer (CIO) has overall responsibility for the GSA IT Security Program. The CIO is responsible for providing guidance, assistance, and management processes to GSA staff and organizations to enable them to perform their responsibilities with regard to GSA's IT Security Program.

1.4.3 Chief Information Security Officer (CISO)

The FISMA establishes the designation of a senior agency information security officer. GSA has assigned this role to the Chief Information Security Officer (CISO). The CISO is the focal point for all GSA IT security and must ensure the security requirements described in this Order are implemented agency-wide. The CISO reports directly to the CIO as required by FISMA.

1.4.4 GSA Senior Agency Official for Privacy (SAOP)

The SAOP is responsible for ensuring GSA's compliance with privacy laws, regulations and GSA policy, and the controls in NIST 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J: Privacy Control Catalog. Within GSA, the CIO is designated as the SAOP.

1.4.5 Heads of Services and Staff Offices (HSSOs)

HSSOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority (e.g., the role of Authorizing Official in writing) to appropriately qualified individuals within their organizations.

1.4.6 Office of CISO Division Directors

OCISO Directors are the intermediary to the AO for ensuring IT security is properly implemented. The Director is the focal point for all IT system security matters for the IT resources under their responsibility.

1.4.7 Authorizing Officials (AOs)

AOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority (e.g., the role of Authorizing Official in writing) to appropriately qualified individuals within their organizations.

1.4.8 Information Systems Security Managers (ISSM)

ISSMs report to the Director of IST in the OCISO. There is at least one ISSM per AO. The ISSM is the focal point for all IT system security matters for the systems under their authority. ISSMs are appointed, in writing, by the Director of IST in the OCISO with concurrence by the CISO. An individual appointed as an ISSM for a system cannot also be assigned as the ISSO for the same system.

1.4.9 Information Systems Security Officers (ISSO)

ISSOs are the focal point for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches. An ISSO must be assigned for every information system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO for a system cannot also be the ISSM for the same system. An ISSO is appointed, in writing, by the Director of IST in OCISO with concurrence by the CISO. An ISSO must be knowledgeable of the information and processes supported by the system.

1.4.10 System Owners (e.g., System Program Managers/Project Managers)

System Owners are management officials within GSA who bear the responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk rests with the System Owners. System Owners must ensure their systems and the data each system processes have the necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM.

1.4.11 Data Owners (e.g., Functional Business Line Managers)

Data Owners are responsible for determining the security categorization of systems based upon Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, levels and ensuring System Owners are aware of the sensitivity of data to be handled. They must coordinate with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA.

1.4.12 Contracting Officers (COs)/Contracting Officer’s Representatives (CORs)

COs/CORs are responsible for coordinating and collaborating with the CISO or other appropriate officials to ensure all agency contracts and procurements are compliant with the agency’s information security policy. They also must ensure the appropriate security and privacy contracting language is incorporated in each contract and task order.

1.4.13 Custodians

Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. They must coordinate with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.

1.4.14 Users of IT Resources

Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA's IT Security Policy and procedures.

1.4.15 System/Network Administrators

System/Network Administrators are responsible for ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.

2 GSA Standard A&A Process

All GSA A&A processes are based upon the NIST SP 800-37 Risk Management Framework. A depiction of the RMF is provided in Figure 2-1.

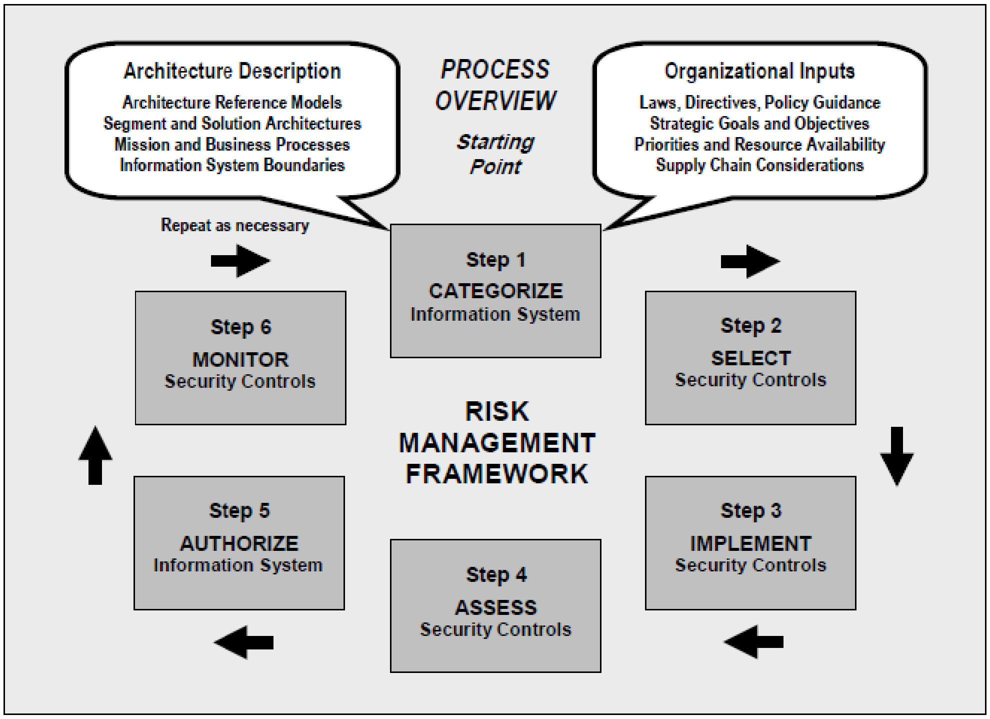

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Figure 2-1. Risk Management Framework (from NIST 800-37)

The Risk Management Framework (RMF) Steps 1-6 associated with the GSA Standard A&A Process are detailed in the following sections. Additional A&A processes GSA has developed or uses are identified in Section 3 which have adapted or modified the standard RMF processes. Documents required as part of a GSA A&A process are listed in Appendix B along with hyperlinks (where available) to document templates.

2.1 RMF Step 1 – Categorize Information System

The first step in GSA's standard A&A process is to determine the FIPS 199 security categorization level of the information system. This level (Low-, Moderate-, or High-impact) will affect the remaining steps in the process. The following tasks detail the actions in RMF Step 1.

TASK 1-1: Security Categorization - Categorize the information system using the GSA FIPS 199 Security Categorization Template (available on the IT Security Forms Page) and document the results of the security categorization in the system security plan (SSP). The System Owner carries out the security categorization process in cooperation and collaboration with appropriate organizational officials with information security/risk management responsibilities including but not limited to the Data Owner, AO, ISSM, and ISSO. The process for determining the appropriate impact level is outlined in FIPS 199 and its companion guides NIST SP 800-60 Volume I, Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories and NIST SP 800-60 Volume II, Revision1, Volume II, Appendices to Guide for Mapping Types of Information and Information System to Security Categories. Please refer to these documents to categorize the information system. The resulting categorization determines the appropriate security control baseline (Low-, Moderate-, or High-impact) for the information system as outlined within NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. The baseline is refined in the GSA NIST 800-53 Control Tailoring Workbook (CTW) to meet GSA's specific needs regarding assignment parameters and applicability of controls.

TASK 1-2: Information System Description - Describe the information system (including system boundary) and document the description in an SSP based on NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems. The SSP provides an overview of the security requirements for the information system, describes the security controls in place or planned for meeting those requirements, and formalizes the plans and expectations regarding the overall functionality of the information system. Descriptive information about the information system is documented in sections 1-12 of the security plan. The level of detail provided in the security plan should be commensurate with the security categorization of the information system. The following sections should be sufficiently detailed:

- Section 2 of the SSP describes the FIPS 199 categorization of the system. The FIPS 199/NIST SP 800-60 analysis must be supported by a completed GSA FIPS 199 Security Categorization Template.
- Section 9 of the SSP describes the function or purpose of the system and its information processes.
- Section 10 of the SSP contains tables outlining the technical system including an inventory of all assets in the authorization boundary. The tables within this section must be completed and depict a complete inventory of hardware, software and operating system components. Any subsystems included in a Major Application (MA) or General Support System (GSS) SSP must be separately identified in an Appendix to the SSP, this appendix will be included as an attachment to the system's ATO Letter.

- Section 11 of the SSP must list all interconnections including the system name, organization, system type (major application or general support system); indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, ATO status, and the name of the AO. Per GSA IT Security Policy 2100.1, "Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the AOs of both systems prior to connecting a system not under a single AO's control in accordance with NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc."

Contact the OCISO at ispcompliance@gsa.gov with questions or requests for further clarification.

TASK 1-3: Information System Registration - Register the information system with the appropriate organizational program/management offices and security personnel. Inform the OCISO, the System/Application ISSM, and the ISSM of the General Support System (GSS) (if different) on which the system will reside and inherit security controls. In addition, each IT system is also an IT investment, which needs to be associated with an IT Investment Portfolio Summary ID (formerly Exhibit 53).

2.2 RMF Step 2 – Select Security Controls

Based on the FIPS 199 impact level (Low-, Moderate-, or High-impact) determined in Step 1, the appropriate controls will be selected from the GSA CTW which also provides the assignment parameters for the applicable NIST SP 800-53 controls. In RMF Step 2, controls will be identified as system-specific, hybrid, or common; controls will be tailored and supplemented (as necessary) with additional controls and/or control enhancements to address unique organizational or system specific risks; a monitoring strategy will be developed; and the AO's approval of the SSP gained.

The following tasks detail the actions in RMF Step 2.

TASK 2-1: Common Control Identification – Leverage the GSA IT FY-15 Information Security Program Plan, Version 1.0 (GSA IT ISPP) to identify the GSA common controls and document them in the SSP initiated in RMF Step 1. Common controls are security controls that are inherited. Common control sources may include the OCISO, OCIO GSSs, S/SO general support systems, and other sources. System Owners inheriting common controls can either document the implementation of the controls in their respective security plans or reference the controls contained in the security plans of the common control providers.

Common control providers are responsible for:

- documenting common controls in a security plan (or equivalent document prescribed by the organization);

- ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization;
- documenting assessment findings in a security assessment report;
- producing a plan of action and milestones for all common controls deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the controls);
- receiving authorization for the common controls from the AO; and
- monitoring common control effectiveness on an ongoing basis.

The Common Control Provider's SSP, Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M) for common controls (or a summary of such information) should be made available to System Owners (whose systems are inheriting the controls) after the information is reviewed and approved by the AO responsible and accountable for the controls.

A Control Summary Table pertaining to its FIPS 199 impact level associated with the system must be completed. The table identifies controls types (common vs. hybrid controls vs. system specific controls) with implementation status (Fully Implemented, Partially Implemented, Planned, etc.) across required controls. The table should be customized to the GSA S/SO or contractor's environment to account for common controls and subsystems (as necessary). Low and Moderate Control Summary Table templates are available for use.

The completed Control Summary table will be included in the appendices section of the SSP. It will be updated in subsequent steps of the RMF process, including after security control implementation and following security assessment to document the results of the review.

TASK 2-2: Security Control Selection - Select the security controls for the information system and document the controls in the SSP. The security controls are selected based on the FIPS 199 security categorization determined in RMF Step 1, Task 1-1, forming the Minimum-security control baseline for the information system. Once the security controls baseline is determined, it must be tailored by applying scoping, parameterization, and compensating control guidance. The tailored baselines, as necessary, can be supplemented with additional controls and/or control enhancements to address unique organizational and/or system specific needs based on a risk assessment (either formal or informal) and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

All systems must complete the GSA NIST 800-53 Control Tailoring Workbook (CTW). The workbook identifies the GSA organizational defined settings. The selected security controls including any controls or enhancements selected above the baseline for the information system will be documented in both the control tailoring workbook and the SSP. A completed Control Tailoring Workbook must be included as an appendix of the system's SSP.

TASK 2-3: Monitoring Strategy - Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation. The developed strategy may follow the RMF Step 6 - Security Control Monitoring process outlined within Section 2.6.1 of this guide, or for systems in GSA's Continuous Monitoring Program, the IT Security Procedural Guide: Information Security Continuous Monitoring Strategy, Chief Information Officer (CIO)-IT Security-12-66. The Continuous Monitoring Plan Template described in this guide may be used by any System Owner to help form an initial plan.

TASK 2-4: Security Plan Approval - Review and approve the security plan. The System Owner shall submit the SSP with the following appendices to the ISSO, ISSM, and the AO:

- Required policies and procedures (as requested by GSA)
- Contingency Plan with a Business Impact Assessment (BIA)
- PIA
- Rules of Behavior (as applicable)
- Interconnection Agreements (as applicable)
- GSA 800-53 CTW
- Control Implementation Summary Table

The OCISO will review SSP package to determine if it is complete, consistent, and addresses the security requirements for the information system. Based on the results of the review, the SSP may require further updating or may be approved. The AO or designated AO representative, by approving the security plan, agrees to the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system; allowing Step 3 of the RMF to begin.

The Security Engineering Division in the OCISO must review and approve the Security Architecture before the system's security controls are implemented. The OCISO Director of IST must accept the SSP before security control implementation activities can begin. Security Plans will be submitted by the System Owner/Program Manager through the ISSO and ISSM to the Director of IST for review.

2.3 RMF Step 3 – Implement Security Controls

Following the approval received in RMF Step 2, implement the security controls specified in the SSP.

The following tasks detail the actions in RMF Step 3.

TASK 3-1: Security Control Implementation - Security control implementation should be consistent with the GSA enterprise architecture and information security architecture. IT systems shall be configured and hardened using GSA IT security hardening guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the AO. Implemented checklists must be integrated with Security

Content Automation Protocol (SCAP) content. Any deviations/exceptions to the hardening guides must be documented and approved by the AO.

To the greatest extent possible, systems are encouraged to conduct initial security control assessments (also referred to as developmental testing and evaluation) during information system development and implementation. Such testing conducted in parallel with the development and implementation of the system facilitates the early identification of weaknesses and deficiencies and provides the most cost-effective method for initiating corrective actions.

TASK 3-2: Security Control Documentation - Document the security control implementation, as appropriate, in the SSP, providing a functional description of the control implementation. The security control implementation descriptions should include planned inputs, expected behavior, and expected outputs (where appropriate) that are typical for technical controls. The SSP should also address platform dependencies and include any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail sufficient to support control assessment in RMF Step 4.

Security controls are documented in Section 13 of the SSP and should be presented in accordance with NIST 800-18. This section must provide a thorough description of how the NIST 800-53 minimum-security controls (Low-, Moderate-, or High-impact) and any supplemental controls are being implemented or planned to be implemented. For each control, descriptions must include:

- the security control title;
- how the security control is being implemented or planned to be implemented;
- any scoping guidance that has been applied and what type of consideration;
- identify the control type (Common, Hybrid, App Specific); and
- identify the implementation status (Implemented, Partially Implemented, Planned, N/A, RBD, etc.), and who is responsible for its implementation.

Note: Systems with multiple components or subsystems must describe control implementations across all components.

2.4 RMF Step 4 – Assess Security Controls

Upon implementation of security controls in RMF Step 3, perform a security control assessment to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Complete the tasks below to determine in place security controls, prepare a SAR, and initiate corrective actions based on the findings and recommendations within it.

The following tasks detail the actions in RMF Step 4.

TASK 4-1: Assessment Preparation - Develop, review, and obtain approval for a Security Assessment Plan (SAP) which will be leveraged to assess the security controls of the information system.

The SAP will provide system background information, the objectives for the security control assessment, the assessment approach, and the assessment test cases to be used in Task 4-2. Review, update, and/or supplement the GSA 800-53 Rev4 Assessment Test Cases. Add additional assessment test cases (from the GSA Assessment Test Cases) for any supplemented controls and/or control enhancements added during Task 2-2, Security Control Selection, to address unique organizational and/or system specific needs. Define the settings deferred to S/SO or contractor recommendation to be reviewed and accepted by the GSA AO.

The following security assessment requirements must be defined in the SAP and implemented for all information systems per its FIPS 199 impact level:

- **FIPS 199 Moderate** and **High** impact systems must be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls.
- **All FIPS 199 Low**, **Moderate**, and **High** impact information systems must conduct authenticated vulnerability scanning of their servers' operating systems as part of security assessment activities. Configuration scans shall be to GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Where a GSA benchmark exists, configuration scanning must be to GSA benchmarks. Any scanning tool configured to support the benchmarks or guidelines identified may be used. Contact OCISO for information on the current tools in use or if there is a question about a specific tool.
- All FIPS 199 Low, Moderate, and High impact information systems with web servers must conduct an authenticated vulnerability scan for the most current Open Web Application Security Project (OWASP) Top Ten Most Critical Web Applications Security Vulnerabilities. Any scanning tool configured to support the OWASP Top 10 may be used. Contact OCISO for information on the current tools in use or if there is a question about a specific tool. If necessary, manual testing and/or verification using the most current OWASP Testing Guide and/or the IT Security Procedural Guide: Web Application Security CIO-IT Security-07-35 is also acceptable. See the GSA IT Security website for links to the OWASP Top Ten Critical Vulnerabilities, the OWASP Testing Guide and the GSA Web Application Security Guide.
- **All FIPS 199 Low**, **Moderate**, and **High** impact information systems with database servers must have their databases assessed as part of their OS vulnerability scanning.
- **All FIPS 199 Low and Moderate** impact Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test (or 'pentest') and provide an Independent Penetration Test Report

documenting the results of the exercise as part of the Assessment and Authorization (A&A) package.

- **All FIPS 199 Low**, **Moderate**, and **High** impact information systems are encouraged (not a requirement) by GSA OCISO to conduct a code analysis using tools to examine the software for common flaws and document results in a Code Review Report, NIST SP 800-53 Control SA-11 enhancement (1).

Note: The 06-30 Scanning Parameter Spreadsheet contains a listing of scanning frequency by technology type and A&A process.

The SAP must be reviewed and approved by the System Owner, ISSO, and ISSM to ensure that the plan:

- includes all appropriate security controls;
- is consistent with system/organizational security objectives;
- employs required assessment tools and techniques;
- provides assessment test cases; and
- outlines automation to support the concept of continuous monitoring and near real-time risk management.

The overall purpose of the SAP approval is two-fold: (i) to establish the appropriate expectations for the security control assessment; and (ii) to bound the level of effort for the security control assessment.

TASK 4-2: Security Control Assessment - Assess the security controls following the SAP and using the GSA Assessment Test Cases updated in Task 4-1 to determine if the controls implemented in RMF Step 3 are operating as intended and producing the desired outcome with respect to meeting the security requirements for the information system.

TASK 4-3: Security Assessment Report (SAR) - Prepare a SAR documenting the issues, findings, and recommendations of the security control assessment. Document the assessment findings with recommendation(s) and risk determinations from the NIST SP 800-30 Rev 1, Guide for Conducting Risk Assessments. Note that this revision of NIST 800-30 expands the risk rating matrix to five levels; Very Low, Low, Moderate, High, and Very High (equivalent to Critical). Findings in the SAR will be addressed in the following manner:

Findings from Test Cases. Each individual finding must be assessed for risk.

Findings from Vulnerability Scans. Individual findings must be identified, however findings may be grouped and assessed by level and type of scan. These findings should be assessed in the following groupings and associated with NIST SP 800-53 control SI-2.

1. Very High (Critical)/High OS/DB Findings
2. Very High (Critical)/High Web Application Findings

3. Moderate OS/DB Findings
4. Moderate Web Application Findings

Findings from Configuration/Compliance Scans. Individual findings must be identified. The findings will be discussed as one group. It will be listed at the Moderate level and associated with NIST SP 800-53 control CM-6.

Low risk findings do not have to be assessed within the SAR; however those findings need to be included in the scan results attached to SAR.

Risk must be determined for findings, as described above, and an overall system or application risk determined. The risk determination will be included as part of the authorization package. Refer to NIST SP 800-30 to ensure that all necessary risk assessment areas are completed.

The risk assessment should consist of the following steps:

- Identifying the list of threats and threat sources to the system. The list should include but not be limited to adversarial outsider and insider threats, accidental user threats, structural threats to its components and facilities, environmental threats to the systems facilities and supporting services;
- Aligning threat sources and events with vulnerabilities;
- Assessing each system instance of absent controls and/or vulnerabilities identified during the security assessment. Evaluate the likelihood the threat sources and events will exploit an identified vulnerability;
- Assess the possible impact to the system and GSA if the vulnerability was exploited;
- Make a determination of risk based on the likelihood the threat will exploit the vulnerability, and the resulting impact, and;
- Evaluate the risks of all identified vulnerabilities to determine an overall level of risk for the system or application.

The SAR must document all findings from the security assessment that are not FULLY SATISFIED with vulnerabilities, threats, an in place controls discussion, likelihood, impact, risk discussion/rating, and recommendations for correcting deficiencies in security controls. Assessment results for subsystems, if any, should be included as a subsection to Section 6 – Findings Discussion of the supporting MA or GSS SAR. If there is more than one subsystem, a separate subsection should be created for each subsystem.

Note: Review and consider ALL risk categories in the process of preparing the final SAR. It is a common mistake to ignore some classes since they are incorrectly believed to be "low risk". However all scanner tools can categorize findings, in much the same way that false positive findings are not real issues, false negative findings or "low/info risk" findings can be real issues, which a human reader will understand are necessarily more important than initially labeled. Moreover low risk items often enhance the risk of other issues or can successfully be combined to generate higher risk. Once identified, they should be rated appropriately in the final SAR.

FIPS 199 Low or Moderate rated systems can possess "High" risk findings the same as High rated systems. All high risk findings must be noted in the SAR.

TASK 4-4: Remedial Action - Conduct initial remediation actions on security controls based on the findings and recommendations of the SAR and reassess remediated control(s), as appropriate. Findings that are remediated should be appropriately marked in the SAR. In the SAR, include ‘‘Resolved” next to the NIST SP 800-53 Control Heading.

2.5 RMF Step 5 – Authorize Information System

Following assessment of the information system in RMF Step 4, the POA&M is prepared based upon the results of the security assessment and any remedial action to correct findings; the Security Authorization Package is assembled and submitted to the AO for adjudication. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable.

Note: GSA tracks all POA&Ms on the POA&M Management Site which serves as the primary tool for the management, storage, and dissemination of GSA system and program POA&Ms.

The following tasks detail the actions in RMF Step 5 – Authorize Information System.

TASK 5-1: Plan of Action and Milestones - Prepare the POA&M from the findings and recommendations in the SAR excluding any remediation actions taken.

Note: External GSA systems and internal GSA systems not being scanning under GSA’s vulnerability scanning program must list all individual findings in their POA&Ms in order to provide GSA OCISO visibility into their vulnerabilities.

Develop the POA&M as follows:

- Do not include vulnerabilities identified as ‘‘Resolved” in the SAR.
- Do not include vulnerabilities identified as Very Low/Low risk. These vulnerabilities still need to be included in the SAR either in relation to a NIST control or in the scan results appendices/attachments.
- Moderate, High, and Very High/Critical risk vulnerabilities need to be included in the POA&M.
    - Assessment findings from test cases become individual entries in the POA&M.
    - Findings based on scans are grouped based on the type of scan, scanned component, and risk level.
        - Vulnerability scan findings will result in one POA&M entry covering all Moderate and High/Very High (Critical) findings on all components. These vulnerabilities will be managed within GSA’s automated scanning tool(s).

- Configuration/Compliance scans may result in a POA&M entry at the Moderate level for all layers scanned as listed in the 06-30 Scanning Parameter Spreadsheet. A POA&M will be created if the scans result in a compliance level of less than 75% for platforms where a GSA hardening guide exists.

The POA&M describes how the System Owner intends to address vulnerabilities (i.e., reduce, eliminate, or accept vulnerabilities). Details on developing POA&Ms are contained in the POA&M procedural guide and on the POA&M site. A GSA POA&M Template is available for personnel with POA&M responsibilities who cannot access the POA&M site. For every Open or Outstanding finding in the SAR, there must be a related planned action in the POA&M for the associated NIST SP 800-53 control or enhancement.

Update the SSP to reflect the results of the security assessment and any modifications to the security controls in the information system. This is necessary to account for any modifications made to address recommendations for corrective actions from the security assessor. Following completion of security assessment activities, the SSP should reflect the actual state of the security controls implemented in the system. Update the GSA 800-53 CTW and applicable Control Implementation Summary Table. The updated documents must be included as appendices to the SSP.

TASK 5-2: Security Authorization Package – The ISSO assembles the security authorization package. The security authorization package includes:

- SSP (with all Appendices and Attachments);
- Security Assessment Report (with all Appendices and Attachments);
- POA&M;
- ATO Letter.

Note: The documents outlined for the Security Authorization Package (above) are required for the GSA Standard A&A Process. The documentation required and links to document templates for other A&A processes GSA uses (and the standard process) are listed in Appendix B.

TASK 5-3: Risk Determination - If an adequate level of information is provided to establish a creditable level of risk, the AO will make a risk level determination. For this determination, the AO assesses all of the information provided by the System Owner as documented in the Security Authorization Package regarding the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks.

TASK 5-4: Risk Acceptance – The explicit acceptance of risk is the responsibility of the AO. The AO determines if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable. Following review of the security authorization package and consultation with key agency officials, the AO must render an authorization decision.

A&A Package Review & Approval. The process for reviewing A&A packages for the GSA standard A&A process is as follows.

> The ISSO assembles the security authorization package and submits it to the ISSM for review. The ISSM will review the package, requesting the ISSO address any inconsistencies/issues. Once satisfied with the package, the ISSM will forward it to the OCISO IST Director.
>
> The OCISO will review the package to provide assurance to S/SO AOs that the systems for which they are responsible have followed required Federal and GSA policy and procedures. Upon completion of this review the OCISO recommends concurrence/non-concurrence to the CISO. The CISO considers this recommendation, collaborates with the AO and others, as necessary, and concurs or non-concurs with granting an ATO based on the security authorization package prior to submitting the ATO Letter to the AO. Concurrences are forwarded to the AO, non-concurrences are returned to the OCISO IST Director.
>
> The AO reviews the completed security authorization package. Based on a determination of the documentation and supporting evidence and whether it establishes an acceptable level of risk the AO may:
>
> - Authorize system operation w/out any restrictions or limitations on its operations;
> - Authorize system operation w/ restriction or limitation on its operations. The POA&M must include detailed corrective actions to correct deficiencies. The ISSM/ISSO must resubmit an updated authorization package upon completion of required POA&M actions to move to full ATO w/out any restrictions; or
> - Not authorize the system for operation.

Note: The System Owner/ISSO must update the SSP and POA&M to reflect any conditions set forth in the ATO letter. Copies of the updated security authorization package including the ATO letter must be distributed to the ISSO, ISSM, System Owner, and the OCISO.

Acceptance of Risk (AOR) Letters. AOR letters are intended for rare or unusual circumstances where the System Owner has limited or no control over the remediation of an identified vulnerability. Examples of such circumstances include:

- Embedded software dependencies
- COTS product update time lines

- Compatibility issues between components

AORs are not intended for delayed or ineffective flaw remediation processes (i.e., patching), insufficient out-year System Development Life Cycle planning (for legacy components), or System Owner preferences. AOR requests must include mitigating factors, compensating controls, and any other action(s) taken to reduce the risk to the system and its data, and a justification for why the vulnerability cannot be resolved. AOR letters have a maximum duration of one year. Upon expiration a new AOR letter may be requested, however it must include new details as to why the vulnerabilities must remain unresolved. AOR letters received without such additional detail will not be approved. Based on the criteria above, AOR letters are:

- Not required for Very Low/Low risk vulnerabilities and findings.
- Required for Moderate risk vulnerabilities and findings. Moderate risk AOR letters require AO approval, but not CISO concurrence.
- Required for Critical/Very High/High risk vulnerabilities and findings. Critical/Very High/High risk AOR letters require AO approval and CISO concurrence.

AOR Letter Processing. AOR letters are processed in the following manner:

1. System Owner/Custodian, ISSO, and ISSM determine the need for an AOR letter based on system POA&Ms.
2. ISSO in conjunction with the ISSM prepares the AOR letter, ensuring an AOR number is added to the footer of the letter.
3. Director of IST notifies the CISO if review and discussions with all stake-holders is appropriate.
4. ISSM submits letter and recommendation to:
   a. AO for approval for Moderate risk vulnerabilities
   b. AO for approval and CISO concurrence for Critical/Very High/High vulnerabilities.
5. Approved document becomes part of the permanent A&A file maintained by the ISSO and ISSM. AOR Letters must be submitted to ISP at ispcompliance@gsa.gov.
6. The ISSO is responsible for monitoring POA&Ms and AOR letters. After one year:
   a. If POA&Ms listed in the AOR letter are still unresolved, a new AOR letter is required with additional details on why the vulnerabilities/findings are unresolved.
   b. If all POA&Ms have been resolved, then the AOR letter is noted as completed and archived as a historical record of the system's A&A status.

A&A Documentation Repository. Upon obtaining a signed ATO Letter, the ISSO will upload a copy of all A&A documentation into the A&A Document Repository. A GSA IT Security Standard Operating Procedure: Assessment and Authorization (A&A) Tracking Process is under development which will be available on the GSA InSite IT Security Procedural Guides webpage when available.

2.6 RMF Step 6 – Security Control Monitoring

2.6.1 Security Control Monitoring

TASK 6-1: Information System and Environment Changes – System Owners must determine the security impact of proposed or actual changes to the information system and its operational environment. Per IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05, proposed system changes must be evaluated to determine potential security impacts. An impact analysis of each proposed change will be conducted using the following as a guideline:

- Whether the change is viable and improves the performance or the security of the system;
- Whether the change is technically correct, necessary, and feasible within the system constraints;
- Whether system security will be affected by the change;
- Whether associated costs for implementing the change were considered; and
- Whether security components are affected by the change.

As outlined within GSA Risk Management Strategy, GSA has a rigorous configuration change management process. The strategy document states that IT changes are requested through a Change Approval Board (CAB) process via a standard CAB form that documents the nature of the change, the criticality, impacts on the user community, testing and rollback procedures, stakeholders, and points of contact. System changes are tested and validated prior to implementation into the production environment. Configuration settings and configuration baselines are updated as necessary to meet new technical and/or security requirements and are controlled through the CAB process.

TASK 6-2: Ongoing Security Control Assessments – System Owners are responsible for assessing a subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with GSA's monitoring strategy. Per IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05, the implemented CM process calls for continuous system monitoring to ensure that systems are operating as intended and that implemented changes do not adversely impact either the performance or security posture of the systems. Per GSA Risk Management Strategy, GSA's Annual Risk Assessments will assess a subset of security controls, common controls that have been identified as weaknesses for GSA systems in past assessments, and other key controls that GSA has identified. Penetration testing and OIG audits may also be performed for a few selected systems as part of an annual assessment.

TASK 6-3: Ongoing Remediation Actions – ISSOs, System Owners, and System, Network, and Database Administrators, will coordinate and perform remediation actions based upon the results of ongoing monitoring activities, assessment of risk, and outstanding items in the system's POA&M. CIO-IT Security-01-05 outlines the implementation of a CM process designed to lower the potential risk to a network by requiring regular "patching" or repairing of known vulnerabilities. CIO-IT Security-01-05 addresses the required steps for implementing changes;

Identifying Changes, Evaluating Change Requests, Decision Implementation, and Implementing Approved Change Requests. Per GSA Risk Management Strategy, risk mitigation shall be the appropriate risk response for all critical and high risks vulnerabilities that can be exploited from the internet and cannot be accepted, avoided, shared, or transferred. Very High/Critical and High risk vulnerabilities must be remediated within thirty (30) days; moderate risk vulnerabilities within ninety (90) days; and low/very low risk vulnerabilities will be addressed on a case-by-case basis. Risk mitigation strategies may include business process improvements, applying timely patches, configuring systems securely, performing secure application code development, and implementing architecture and design modifications as necessary. Risk mitigation measures will be employed based on prioritization. Some of the risk prioritization assessment criteria may include the probability of vulnerability exploitation, material business impact if vulnerability is successfully exploited, compliance requirements, cost and business impact of remediation activities and controls.

TASK 6-4: Key Updates – The System Owner and ISSO will update the following items as part of the system and GSA continuing monitoring plans, processes, and program.

- SSP (and all appendices and attachments)
- SAR (and all appendices and attachments)
- POA&M

The updates will be based on regular updates required by GSA processes, such as:

- Weekly/Monthly/Quarterly vulnerability scans from GSA's scanning program
- Annual FISMA Self-assessments
- Changes identified as part of the system's CM Plan
- Changes identified as part of the system's ConMon Plan.

As part of the CM process outlined within CIO-IT Security 01-05, security testing will be conducted following major or significant system changes. If the changes introduce vulnerabilities, actions to mitigate the vulnerabilities must be included in the system's POA&M, per GSA's POA&M management process, for tracking of the resolution. The SSP will be updated to reflect any changes.

TASK 6-5: Security Status Reporting - The System Owner and ISSO will report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate organizational officials on an ongoing basis. GSA's vulnerability scanning program, the GSA POA&M management process, and any required reporting programs will be used to provide security status reporting. AOs and other personnel with security related responsibilities will leverage these resources to keep apprised of the risk levels associated with their system(s).

TASK 6-6: Ongoing Risk Determination and Acceptance – The System Owner, AO, and ISSO will review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with GSA's continuous monitoring strategy and the system's continuous monitoring plan to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation (where applicable) remains acceptable. Data reported via GSA's vulnerability scanning program, the GSA POA&M management process, annual assessments, and other assessment processes (e.g., Penetration Testing, audits, FISMA metrics) will be used by the AO to determine the acceptance of risks and the need to perform reauthorization.

TASK 6-7: Information System Removal and Disposal – System Owners and ISSOs will establish a disposal plan in accordance with NIST SP 800-64 Security Considerations in the Information System Development Life Cycle, GSA Order CIO 2140.3, Systems Development Life Cycle (SDLC) Policy, and the GSA Solutions Life Cycle Handbook. In support of this plan, system owners will document the transfer and/or disposal of GSA IT Systems under the provisions outlined within CIO 2100.1, Chapter 3, Section 2.d and IT Security Procedural Guide: Media Protection, CIO-IT Security-06-32.

2.6.2 Information Security Continuous Monitoring Strategy

Inventoried GSA systems that have attained an ATO may request entrance into GSA's Information Security Continuous Monitoring Program. Systems the meet the qualifying requirements of this this program no longer follow the three (3) year security authorization process for GSA information systems. New systems must continue to follow one of the GSA A&A processes to obtain a full three year ATO, including re-authorization every three years, when the system undergoes a significant change or when there is a major security breach impacting the security posture of the system. Specific requirements for admittance into the Information Security Continuous Monitoring Program are detailed in the CIO-IT Security 12-66.

2.6.3 Security Authorization Process Guidance for Significant Changes

Significant changes as defined in NIST SP 800-37, Appendix F, Page F-7 require reauthorization following the security authorization process requirements in this guide. Contact the OCISO at ispcompliance@gsa.gov to determine the scope of reauthorization activities.

2.6.4 Security Authorization Process Guidance for Expiring Authorizations

ISSOs with assistance from ISP can track the expiration dates of ATOs. Renewal of ATOs are initiated by the Authorizing Officials, ISSMs and ISSOs. Per GSA CIO 2100.1 e. (5), *"Information systems with expiring Authorizations to Operate (ATO) may request a one-time extension of the current authorization for a period not to exceed one year from the date of ATO expiration if during this time the system will be decommissioned or to allow development of near real-time continuous monitoring capabilities to support ongoing authorization. ATO extensions must be supported by current vulnerability assessment results (operating system, database, and web (as applicable)) and POA&M identifying weaknesses from all sources. AOs must obtain approval from the CISO for the continuous monitoring plans of systems authorizations that have been extended. Plans must be approved within 6 months of the extension."*

Questions concerning the security authorization process, significant changes, or expiring ATOs can be directed to ispcompliance@gsa.gov.

3 Security Authorization Process

In addition to the GSA Standard A&A Process, GSA has implemented several other A&A processes for the purpose of ensuring risks to GSA IT resources are reduced to the extent possible based on budget constraints, business requirements and other resource issues. These processes and the criteria required for each are outlined below. The specific details describing each of the processes may be found in the document listed in "Document Reference" in Section 3.2 for each assessment type. Regardless of which A&A process is followed, before assessment activities for information systems begin, the following requirements must be met:

(1) The SSP is approved.

(2) The information system's architecture is approved by the OCISO Security Engineering Division (ISE).

(3) The SAP is approved.

3.1 Identifying the Appropriate A&A Process/Program

Table 3-1 identifies the criteria to qualify for each A&A process.

Table 3-1. A&A Process Requirements

A&A Process/Program	Qualifying Criteria
Standard GSA Process	• All new and existing GSA information systems that do not fall under one of the other A&A processes
Lightweight Security Authorization Process	• New GSA information systems pursuing an agile development methodology • Reside on infrastructures that have a GSA ATO concurred to by the CISO or a Federal Risk and Authorization Management Program (FedRAMP) ATO • Must be FIPS 199 Low or Moderate
GSA Salesforce Process	• Applicable to applications that integrate into the main Salesforce.com application and are hosted on Salesforce.com's infrastructure • Applications developed for internal and external GSA use published on the Salesforce Platform
Security Reviews for Low Impact Software as a Service Solutions Process	• Private sector cloud computing Software as a Service (SaaS) solutions that are implemented within GSA • Duration is limited and/or one time use • Data already exists in the public domain or data is non-sensitive and is considered FIPS 199 low impact • GSA would not be harmed regardless of the consequence of an attack or compromise • Dollar cost for such deployments do not exceed $100,000 annually

A&A Process/Program	Qualifying Criteria
GSA Agency FedRAMP Process	• A Cloud Service Provider (CSP) requesting GSA Agency sponsorship into FedRAMP • GSA accepts sponsoring the CSP • GSA determines CSP's security authorization package will be considered FedRAMP compliant
Security Reviews for Moderate Impact Software as a Service Solutions Process	• Dollar cost for such deployments do not exceed $100,000 annually • Must be FIPS 199 Moderate • Vendor has had an external assessment done such as a SOC 2/SSAE 16 or FedRAMP approval within the past year • If not FedRAMP approved, must be enrolled in the FedRAMP certification process
GSA Subsystem Process	• Classified as a subsystem (and not a Salesforce application) • Majority of it security controls provided by the GSS/MA in which it operates • FIPS 199 Low or Moderate • FIPS 199 level can be below the level of the host GSS or MA
GSA Continuous Monitoring Program	• Must be an inventoried GSA system with an ATO • Underlying GSS must be in GSA's continuous monitoring program (contact OCISO if this criteria is a roadblock) • Has implemented automated continuous monitoring capabilities • SSP and POA&M up to date • Develop a Continuous Monitoring Plan

3.2 A&A Process Descriptions

Additional details about the GSA A&A processes listed in Table 3-1 are provided in the following sections:

3.2.1 GSA Standard A&A Process

- **Document Reference**: Throughout this guide, process steps are described in Section 2.
- **Result**: Full 3 Year ATO
- **Summary of Process**: All new and existing GSA information systems must undergo a security assessment and authorization at least every three (3) years or whenever there is a significant change to the system's security posture. The result is an ATO for a period not to exceed three (3) years. Specific requirements are detailed throughout this guide.
- **A&A Package Review & Approval Process**: Follows the process described in Section 2.5.

3.2.2 Lightweight Security Authorization Process

- **Document Reference:** IT Security Procedural Guide: Lightweight Security Authorization Process" (GSA CIO IT Security 14-68)
- **Result:** Limited ATO (LATO) - Initial 90 day/1 Year (Moderate), Full 3 Year ATO (Low)

- **Summary of Process:** New GSA information systems pursuing an agile development methodology AND residing on infrastructures that have a GSA ATO concurred by the GSA Chief Information Security Officer (CISO) or a FedRAMP ATO. The process allows for an initial 90-day LATO for Low and Moderate pilot systems to support integration, testing, and limited production capabilities (as defined by the GSA CISO) that can be extended to a one year LATO for FIPS 199 Moderate impact systems and a full three-year ATO for FIPS 199 Low impact information systems in the GSAIT organization.

  A LATO comes in two forms, an initial 90-day LATO and a 1 year LATO. The initial 90-day LATO is based on a 2 week assessment that begins upon satisfactory completion and sign-offs of sections 1-12 of the SSP. Assessment activities will commence following approval of the SSP. Assessment activities will include:

  - Unauthenticated external vulnerability scanning
  - Unauthenticated external web application scanning
  - External Gray-box penetration testing

  External vulnerability and web application scanning will be conducted by the OCISO Security Operations Division (ISO) while Penetration Testing will be conducted by the OCISO Services and Staff Offices ISSO Support Division (IST). Assessment activities will take one (1) week and will result in a Penetration Test Report. The Penetration Test Report together with the SSP, POA&M, and ATO memoranda's will form the basis for the initial 90-Day LATO Package. The package with exception of the Penetration Test Report will be prepared by the supporting ISSO.

  The initial 90-Day LATO can be extended to a one year LATO for FIPS 199 Moderate impact systems and a full three-year ATO for FIPS 199 Low impact information systems in the GSAIT organization following the process detailed in the Lightweight Security Authorization Procedural Guide.

- **A&A Package Review & Approval Process**: Follows the process described in Section 2.5.

3.2.3 GSA Salesforce Platform Process

- **Document Reference:** IT Security Procedural Guide: GSA's Security Implementation of the Salesforce Platform (GSA CIO IT Security 11-62)

- **Result:** Salesforce Application ATO

- **Summary of Process**: Specific to applications developed for internal and external GSA use published on the Salesforce Platform. The first step is to determine the type of application. If the application is a Major Application, then a full Assessment and Authorization is required. If the application is a Subsystem, there are key activities that should be completed. Applications are assessed and authorized in accordance with this guide, Salesforce Organization Baseline Security Configuration Settings, and specific requirements detailed in GSA's Security Implementation of the Salesforce Platform Procedural Guide.

- **A&A Package Review & Approval Process**: After the ISSM accepts/approves the A&A package it is forwarded to the CISO for signature (i.e., no OCISO Director review).

3.2.4 Security Reviews for Low Impact Software as a Service Process

- **Document Reference:** IT Security Procedural Guide: GSA CIO IT Security 16-70, *Security Reviews for Low Impact Software as a Service (SaaS) Solutions* has been developed and will be available on the GSA InSite IT Security Procedural Guides webpage when posted.

- **Result:** 1 year ATO or less

- **Summary of Process:** Private sector cloud computing Software as a Service (SaaS) solutions that are implemented within GSA for (1) limited duration and/or one time use; (2) involve data already in the public domain or data that is non-sensitive and could be considered FIPS 199 low impact, (3) GSA would not be harmed regardless of the consequence of an attack or compromise; and, (4) if the dollar cost for such deployments do not exceed $100,000 annually. AOs must consider Federal and agency information security requirements, and the S/SO security needs. An evaluation of the data and project scope must be performed to assure the conditions noted above are met. A review of the security controls and activities for such systems must be performed to assure the security controls and practices of the contractor are adequate before authorizing use and accepting residual risk. The ATO shall only be valid for the period of the time the application license is valid or one (1) year, whichever is shorter.

- **A&A Package Review & Approval Process**: Follows the same process described in Section 2.5, with the following exceptions; (1) the Director of ISP replaces the Director of IST for the review and further processing of the A&A package, (2) the CISO is the final signature on the ATO letter—no AO signature.

3.2.5 FedRAMP Process

Document Reference: Guide to Understanding Federal Risk and Authorization Management Program (FedRAMP), additional details available at FedRAMP Review & Approve Process and FedRAMP Standard Operating Procedures & Checklists

- **Result:** FedRAMP ATO (Agency)

- **Summary of Process:** A Cloud Service Provider (CSP) may elect to request an Agency FedRAMP ATO from GSA. It is at the discretion of GSA to accept or deny the CSP's request for sponsorship. CSPs which GSA agrees to sponsor a FedRAMP authorization are required to follow the FedRAMP PMO authorization process requirements. GSA has defined assignments for NIST SP 800-53 control parameters within the FedRAMP Low and Moderate baselines as its organizationally defined parameters. The parameters are contained in Appendix C. Additional information about FedRAMP is available in the reference documents and at http://www.fedramp.gov. The CSP must provide a security authorization package to GSA. If GSA determines the package to be FedRAMP compliant the CSP in cooperation with GSA will pursue a FedRAMP ATO.

System Owners/AOs with questions about leveraging the FedRAMP security authorization process (to attain a Government wide authorization) should contact the OCISO at ispcompliance@gsa.gov.

- **A&A Package Review & Approval Process**: Follows the FedRAMP process.

3.2.6 GSA Moderate Software as a Service (SaaS) Solutions Process

- **Document Reference:** IT Security Procedural Guide: GSA CIO IT Security 16-71, *Security Reviews for Moderate Impact Software as a Service (SaaS) Solutions* has been developed and will be available on the GSA InSite IT Security Procedural Guides webpage when posted.

- **Result:** 1 Year ATO

- **Summary of Process:** Specific to applications: (1) the dollar cost of such deployment does not exceed $100,000 annually, (2) determined to be FIPS-199 Moderate impact system, (3) data center security is qualified by a current Standards for Attestation Engagements (SSAE) 16/ Service Organization Control (SOC) 2, or Federal Risk and Authorization Management Program (FedRAMP) approval, must be enrolled in the FedRAMP certification process. AOs must consider Federal and agency information security requirements, and the S/SO security needs. An evaluation of the data and project scope must be performed to assure the conditions noted above are met. A review of the security controls and activities for such systems must be performed to assure the security controls and practices of the contractor are adequate before authorizing use and accepting residual risk. The ATO shall only be valid for one (1) year. Approved Moderate SaaS applications become subsystems of the Enterprise Cloud Services (ECS) General Support System (GSS).

- **A&A Package Review & Approval Process**: Follows the same process described in Section 2.5, with the following exceptions; (1) the Director of ISP replaces the Director of IST, (2) the CISO is the final signature on the ATO letter—no AO signature.

3.2.7 GSA Subsystem Process (previously Minor Application Process)

- **A&A Process Reference:** Described within this section.

- **Result:** Aligned with subsystem's GSS or MA ATO.

- **Summary of Process:** This process is specific to subsystems (other than Salesforce applications) categorized with a FIPS 199 security impact level of Low or Moderate , dependent upon the resources provided by its underlying GSS or MA, with the underlying GSS or MA providing the majority of the subsystem's security controls. The supporting GSS or MA must be shown to provide a foundational level of protection for the subsystem; the subsystem may have a FIPS 199 level equal to or below the level of the host GSS or MA.

Subsystems with a FIPS 199 security impact level of Low will adhere to and implement the controls per the Lightweight Security Authorization Process Procedural Guide.

Subsystems with a FIPS 199 security impact level of Moderate will document in a subsystem SSP all controls identified as hybrid or system specific by the underlying GSS or MA. These controls will be assessed using GSA NIST 800-53 Test Cases and the results shared with the underlying GSS/MA System Owner/ISSO. All subsystems will be identified in an Appendix of their host GSS/MA's SSP which will also be attached to the GSS/MA's ATO Letter. All subsystems inherit its GSS/MA's ATO cycle.

- **A&A Package Review & Approval Process**: Subsystems are included in the A&A Package Review & Approval Process of their host GSS/MA. No separate ATO is issued for subsystems.

3.2.8 GSA Continuous Monitoring Program

- **A&A Process Reference:** IT Security Procedural Guide: Information Security Continuous Monitoring Strategy CIO-IT Security-12-66
- **Result:** Continuous Monitoring Ongoing Authorization
- **Summary of Process:** The GSA Continuous Monitoring Program replaces the three (3) year security authorization process for GSA information systems that meet its qualifying requirements with an ongoing authorization process. The GSA Continuous Monitoring baseline controls are assessed in two ways; (1) Controls identified as automated will be verified via both self-attestation and enterprise-level oversight performed by the OCISO using reports and feeds generated using automated tools, (2) Manual controls or process-based controls are vetted via either self-attestation or self-attestation with supporting deliverable. All self-attestations are due annually together with the annual FISMA assessment and continuous monitoring plan update. In cases where security controls are determined to be inadequate, the continuous monitoring program facilitates prioritized security response actions based on risk.
- **A&A Package Review & Approval Process**: Follows the same process described in Section 2.5, with the following exception, the Director of ISP replaces the Director of IST.

4 GSA Implementation of CA, PL, and RA Controls

NIST SP 800-53 defines controls related to the security authorization process that GSA is required to implement based on an information system's security categorization. The Security Assessment and Authorization (CA), Planning (PL), and Risk Assessment (RA) control family implementations are addressed in this guide.

Note: The GSA IT ISPP was developed to provide stakeholders with detailed information on the NIST controls GSA has considered inheritable common and hybrid controls and who the responsible party is for implementing the control. In the following sections when a control implementation is covered in the ISPP the control's subsection will refer to the ISPP for parameter assignments and implementation guidance.

4.1 Security Assessment and Authorization (CA)

4.1.1 CA-1 Security Assessment and Authorization Policy and Procedures

Parameter assignments and implementation guidance for the CA-1 control are provided in the ISPP.

4.1.2 CA-2 Security Assessments

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
    1. Security controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine security control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system and its environment of operation [*Annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to [Information System Security Manager, Information System Security Officer, System Owners (aka System Program Managers, System Project Managers, Acquisitions/Contracting Officers, Custodians)].

Control Enhancements:

(1) The organization employs assessors or assessment teams with [The use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls. To achieve impartiality, assessors should not: (i) create a mutual or conflicting

interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.] to conduct security control assessments

(2) The organization includes as part of security control assessments, [Annual], [Announced], [Penetration Testing].

GSA Implementation Guidance:
GSA requires security control assessment to be performed for all information systems as part of the security authorization/re-authorization process. The security control assessment must include the GSA NIST 800-53 assessment test cases. The security control assessment must document the implementation status in sufficient detail in order to assist in determining the overall effectiveness of all controls and enhancements that have been selected and implemented for the system as per FIPS-199 impact level.

GSA's process for performing a security control assessment is fully defined in Section 2.4 of this guide, RMF Step 4 – Assess Security Controls. The results of the security control assessment must be documented in a SAR.

As per CA-2, Enhancement (1), GSA FIPS 199 Moderate and High Impact Systems must be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls.

CA-2, Enhancement (2), requires GSA FIPS High Impact Systems to be assessed annually, via announced penetration tests. Penetration testing provides a more thorough analysis of the implementation effectiveness for both physical and technical security controls associated with an information system.

Additional Contractor System Considerations: *None.*

4.1.3 CA-3 System Interconnections

Control: The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements [*At least annually*].

Control Enhancements:

(5) The organization employs [*deny-all, permit-by-exception*] policy for allowing [*all GSA systems*] to connect to external information systems.

GSA Implementation Guidance:

The focus of this control is to ensure that any persistent connection to any other information system outside of the system's authorization boundary has been approved by the AO, identified and documented within the SSP, and monitored on an ongoing basis.

Chapter 3 of GSA CIO 2100.1 outlines the following interconnection requirements:

Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the AOs of both systems prior to connecting a system not under a single AO's control in accordance with NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems." Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc.;

If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system; and

All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the GSA CISO.

The terms "connection" or "interconnection" in this case, means any on-going, persistent or substantial interaction with any information system(s) that is located outside of the authorization boundary. These connections can be physical and/or logical, and include data entering or exiting to/from the authorization boundary. User-controlled connections such as email, ftp, remote access, and web browsing are not considered interconnections and therefore do not apply to this control.

Additional Contractor System Considerations: None.

4.1.4 CA-5 Plan of Action and Milestones

Control: The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones [*quarterly*] based on the findings from security impact analyses, and continuous monitoring activities.

GSA Implementation Guidance:
The focus of this control is to ensure that all information systems have developed a Plan of Action and Milestones in accordance with the GSA IT Security Procedural Guide: Plan of Action and Milestones (POA&M) CIO-IT Security-09-44 which details the POA&M processes and procedures for meeting the requirements of this control.

A quarterly POA&M report must be submitted to the OCISO in order to monitor agency-wide remediation efforts as required by OMB policy. These updates must be performed for each quarter of the fiscal year using the GSA POA&M workbook which is maintained by the system ISSO or ISSM and uploaded to the GSA FISMA POA&M Management Site for OCISO review. The POA&M Management Site serves as the primary page for managing and communicating GSA's system and program POA&Ms, and is available internally at GSA, or from the web via VPN. New systems that are currently undergoing security authorization process or that have not been included in the GSA FISMA inventory must use the POA&M Template available on GSA InSite.

Additional Contractor System Considerations:
Contractor systems must submit POAMs through their Government ISSO(s) as contractors will not have access to the POA&M Management Site. Government ISSOs supporting these systems must facilitate POA&M updates by sending the current version of the system POA&M together with the quarterly OCISO guidance to the contractor representative(s). Upon receipt of the POA&M from the contractor, Government ISSOs shall review the POA&M to ensure it is updated and includes required vulnerabilities, before posting the POA&M to the GSA POA&M Management Site.

4.1.5 CA-6 Security Authorization

Control: The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization [Every three (3) years or when a significant change occurs as defined in NIST SP 800-37, Appendix F, Page F-7].

GSA Implementation Guidance:
The focus of this control is to ensure that all information systems which have been authorized to operate before being placed into operational status. All information systems must undergo authorization/reauthorization every three years or when there is a significant change as defined in NIST SP 800-37, Appendix F, Page F7 following the security authorization process documented in this guide. Detailed procedures for the security authorization process can be found in Section 2.5 of this guide, RMF Step 5 – Authorize Information System. Additional ATO or authorization types exist in GSA and are described in Section 3.2 of this document.

The explicit acceptance of *risk* is the responsibility of the AO. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing the security authorization package submitted by the System Owner. The security authorization package provides the AO with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

The security authorization package includes:

- SSP (required policies and procedures (as requested by GSA), Rules of Behavior, Interconnection Agreements (as applicable), GSA 800-53 Control Tailoring Workbook, and appropriate Control Implementation Summary Table);
- Security Assessment Report (w/ required appendices (see Appendix B));
- POA&M;
- Independent Penetration Test Report;
- Code Review Report (Strongly Recommended);
- Contingency Plan;
- Contingency Plan Test Report; and
- ATO Letter.

The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable. Following review of the security authorization package and consultation with key agency officials, the AO must render an authorization decision to:

- Authorize system operation w/out any restrictions or limitations on it operation;
- Authorize system operation w/ restriction or limitation on its operation. The POA&M must include detailed corrective actions to correct deficiencies. Resubmit an updated security authorization package upon completion of required POA&M actions to move to ATO w/out any restrictions; or
- Not authorized for operation.

Questions concerning the security authorization process, significant changes, or CIO 2100.1 can be directed to ispcompliance@gsa.gov.

Additional Contractor System Considerations: *None.*

4.1.6 CA-7 Continuous Monitoring

Parameter assignments and implementation guidance for the CA-7 control are provided in the ISPP.

CIO IT Security 12-66 provides detailed information on the implementation of GSA's Information System Continuous Monitoring Program.

4.1.7 CA-8 Penetration Testing

Control: The organization conducts penetration testing [*annually*] on [*all FIPS 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test*.]

Control Enhancements:

(1) The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

GSA Implementation Guidance:

All FIPS 199 Low and Moderate impact Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Annual penetration tests can be completed internally and do not require an independent assessor.

Additional Contractor System Considerations: *None.*

4.1.8 CA-9 Internal System Connections

Control: The organization:

a. Authorizes internal connections of [*If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system*] to the information system; and
b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

GSA Implementation Guidance:
If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system

4.2 Planning (PL)

4.2.1 PL-1 Security Planning Policy and Procedures

Parameter assignments and implementation guidance for the PL-1 control are provided in the ISPP.

4.2.2 PL-2 System Security Plan

Control: The organization:

a. Develops a security plan for the information system that:

1. Is consistent with the organization’s enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Information System Security Manager, Information System Security Officer, System Owners (aka System Program Managers, System Project Managers, Custodians)*];

c. Reviews the security plan for the information system [*Annually*];

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

Control Enhancements:
(3) The organization plans and coordinates security-related activities affecting the information system with [*Information System Security Manager, Information System Security Officer, System Owners (aka System Program Managers, System Project Managers, Custodians)*] before conducting such activities in order to reduce the impact on other organizational entities.

GSA Implementation Guidance:
The focus of this control is to ensure that a SSP has been developed for the information system that documents the security requirements for the information system, and the implementation status of the security controls that have been assigned to the system as per FIPS 199 impact analysis. All GSA information systems must develop a SSP in accordance with this guide and NIST SP 800-18. Detailed guidance is available in sections RMF Step 1 – Categorize Information System and RMF Step 3 – Implement Security Controls of this guide, as well as in the GSA A&A Package Review Standard Operating Procedure.

The security requirements per FIPS-199 impact level and the security controls which are planned or in-place to meet these requirements, must be documented within the SSP and updated as-needed to reflect any change to the information system environment. Updates made to the SSP must include updates to system applications and hardware, remediation of previously identified weaknesses and any addition of new weaknesses identified through security assessments or continuous monitoring.

Additional Contractor System Considerations: *None.*

4.2.3 PL-4 Rules of Behavior

Parameter assignments and implementation guidance for the PL-4 control are provided in the ISPP.

4.2.4 PL-8 Information Security Architecture

Control: The organization:

a. Develops an information security architecture for the information system that:

    1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
    2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
    3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture [At least Annually] to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

GSA Implementation Guidance:
Reviews and updates the information security architecture annually to reflect updates in the enterprise architecture; Security Engineering Framework requires every system seeking authorization to have their architecture approved by ISE before beginning security assessment activities.

4.3 Risk Assessment (RA)

4.3.1 RA-1 Risk Assessment Policy and Procedures

Parameter assignments and implementation guidance for the RA-1 control are provided in the ISPP.

4.3.2 RA-2 Security Categorization

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

GSA Implementation Guidance:
GSA system owners, data owners, ISSOs, and ISSMs are required to follow the processes and procedures described in Section 2.1 of this guide for determining the security categorization their information and information systems.

Additional Contractor System Considerations: *None*

4.3.3 RA-3 Risk Assessment

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in [*Security Assessment Report (SAR*)];
c. Reviews risk assessment results [*Every three (3) years or with a significant change as defined in NIST SP 800-37 rev 1, Appendix F, Page F-7*]; and
d. Disseminates risk assessment results to [*Information System Security Manager, Information System Security Officer, System Owners (aka System Program Managers, System Project Managers, Custodians)*]; and
e. Updates the risk assessment [*Every three (3) years or with a significant change as defined in NIST SP 800-37 rev 1, Appendix F, Page F-7*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

GSA Implementation Guidance:
The focus of this control is to verify that an assessment of risk is performed and documented for the information system and that the subsequent security assessment report is communicated to GSA senior management, in order to provide key information regarding the system's current security state and resulting risk to GSA operations, assets, and individuals. The results of the risk assessment provide critical information to assist the GSA AO in determining whether or not to authorize/re-authorize the information system.

GSA requires a risk assessment to be conducted as part of the initial security authorization process, then every three years or whenever a significant change occurs as defined in NIST SP 800-37, Appendix F, Page F7. GSA's process for performing a risk assessment is fully defined in Section 2.4 of this guide. The results of this risk assessment must be documented in the SAR template.

Additional Contractor System Considerations: *None*

4.3.4 RA-5 Vulnerability Scanning

Parameter assignments and implementation guidance for the RA-5 control are provided in the ISPP.

5 Summary

Managing enterprise-level risk through a system life cycle perspective is a departure from the traditional view of security authorization as a static, procedural process. The policies and procedures outlined in this guide provide an effective approach to system security authorization that is more dynamic and more capable of managing information system-related security risks across a diverse enterprise.

This guide describes GSA's agency-wide security authorization processes in accordance with NIST Risk Management Framework and the security authorization process as described in NIST SP 800-37.

All GSA information systems must undergo security control assessment and be authorized to operate according to their specific process, GSA's standard A&A process requires A&A at least every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST SP 800-37.

GSA contractors and Federal employees should use this guide and the noted references prior to selecting and performing a security authorization process. Where there is a conflict between NIST guidance and GSA guidance, contact OCISO at ispcompliance@gsa.gov.

Appendix A: Consolidated List of Guidance, Policies, Procedures

Federal Guidance:

- NIST Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Revision 1
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4
- FIPS 199, Standard for Security Categorization of Federal Information and Information Systems
- NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1
- NIST SP 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1

GSA Guidance:

- GSA Information Technology (IT) Security Policy (CIO 2100.1)
- GSA IT Security Procedural Guide: Managing Enterprise Risk – Security Assessment and Authorization, Planning and Risk Assessment (GSA CIO IT Security 06-30)
- GSA IT Security Procedural Guide: Lightweight Security Authorization Process (GSA CIO IT Security 14-68)
- GSA IT Security Procedural Guide: GSA's Security Implementation of the Salesforce Platform (GSA CIO IT Security 11-62)
- GSA IT Security Procedural Guide: Continuous Monitoring Program (CIO IT Security 12-66)
- GSA IT Security Procedural Guide: IT Security Program Management Implementation Plan (CIO-IT-Security 08-39)
- GSA IT Security Procedural Guide: Security Language for IT Acquisition Efforts (CIO-IT-Security 09-48)
- GSA IT Security Procedural Guide: Security Review for Low Impact Software as a Service (SaaS) Solutions (CIO-IT-Security 16-70)
- GSA IT Security Procedural Guide: Security Review for Moderate Impact Software as a Service (SaaS) Solutions (CIO-IT-Security 16-71)

Appendix B: A&A Process Package Document Lists/Links

This Appendix contains a listing of the A&A Package documentation requirements for each of the A&A processes described in this guide, where possible hyperlinks to applicable documents and templates have been provided.

Standard A&A Process
Documents
System Security Plan Appendix A - Acronyms, Terms, and Definitions Appendix B - References Appendix C - Hosted Subsystems (if applicable) Other Appendices, as necessary Attachment 1: Privacy Impact Assessment Attachment 2: FIPS 199 Security Categorization Attachment 3: e-Authentication Assurance Level Attachment 4: Interconnection Security Agreement(s)/Memoranda of Understanding Attachment 5: GSA NIST 800-53 Control Tailoring Workbook (CTW) Attachment 6: Control Summary Table (based on FIPS 199 Categorization) Low Control Summary Table Moderate Control Summary Table Attachment 7: Contingency Plan (based on FIPS 199 Categorization) CP Plan for Low Impact System CP Plan for Moderate Impact System Attachment 8: Contingency Plan Test Report Attachment 9: Incident Response Plan Attachment 10: Incident Response Plan Test Report Attachment 11: Configuration Management Plan Attachment 12: Continuous Monitoring Plan (if applicable) Attachment 13: Rules of Behavior (if applicable) Attachment 14: Code Review Report (if applicable) Other Attachments, as necessary
Security Assessment Report (Results from the Security Assessment Plan) Appendix A - Acronyms, Terms, and Definitions Appendix B - GSA NIST 800-53 Security Assessment Test Cases Appendix C - Operating System Scanning Results Appendix D - Database Application Scanning Results Appendix E - Web Application Scanning Results Other Appendices, as necessary Attachment 1: Penetration Test Report Other Attachments, as necessary
Plan of Action and Milestones (POA&M)
ATO Letter

Lightweight Security Authorization Process
Documents
System Security Plan Lightweight Process System Security Plan for Amazon Web Services (AWS) Lightweight Process System Security Plan for CGI Federal IaaS Cloud
Security Assessment Report Lightweight Security Assessment Report - AWS Lightweight Security Assessment Report - CGI
Select GSA NIST 800-53 Security Assessment Test Cases AWS Security Assessment Test Cases CGI Federal IaaS Cloud Security Assessment Test Cases
Customer Responsibility Matrix AWS Federal IaaS Cloud Customer Responsibility Matrix CGI Federal IaaS Cloud Customer Responsibility Matrix
OS, Web App, Database Scan Data
Penetration Test Report
ATO Letter

GSA Salesforce Process
Documents
IT Security Procedural Guide: GSA's Security Implementation of the SalesForce Platform, CIO-IT Security-11-62 contains templates or instructions concerning its required A&A package where hyperlinks are not provided below.
PIA
Security Control Analysis
Application Configuration Document
Code Scan Reviews
SalesForce Application Review Document
Plan of Action and Milestones (POA&M)
ATO Letter

Security Reviews for Low Impact Software as a Service Solutions Process
Documents
IT Security Procedural Guide: Security Reviews for Low Impact Software as a Service (SaaS) Solutions (GSA CIO IT Security 16-70) has been developed and will be available on the GSA InSite IT Security Procedural Guides webpage when posted. Once posted, refer to it for the documents required in A&A Packages, until that time contact the OCISO for guidance. At a minimum the documentation listed below is required.
Documented results of required review activities, including:
Assign a unique ID to each person. Users must be individually identified (Reference NIST SP 800-53 control IA2 - Identification and Authentication).
Document and implement system and security parameters deferred to customers. Do not use the vendor-supplied defaults for system passwords and other security parameters.
All transmissions of authentication credentials must be encrypted (e.g., TLS over HTTPS). It is strongly recommended that the entire session be encrypted.
Web application scanning results (e.g., WebInspect, Acunetix, Burp Suite Pro, etc.).
Operating System vulnerability scanning results (e.g., Nessus, Qualys, nCirlce, McAfee

Vulnerability Manager, etc.). Scans are not necessary for vendors that are PCI DSS Compliant or that have a McAfee Secure Seal or TrustGuard Quarterly Scanned Seal. Vendors that are PCI DSS Compliant or have the McAfee Secure Seal or TrustGuard Quarterly Scanned Seal must provide the results of their latest scan.
Verify that the vendor has an acceptable flaw remediation process. Vendors must be able to identify and remediate information system flaws in a timely manner (i.e., how often scans are completed and how vulnerabilities are remediated). Reference NIST 800-53 R4 control SI2 – Flaw Remediation.
The site must have an acceptable "terms of service" approved by the GSA legal office.
Vendor shall either provide the results of their Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 16 audit report and/or have one of the following vendor certifications SysTrust, WebTrust (American Institute of Certified Public Accountants (AICPA)-sponsored), ISO/IEC 27001, or PCI DSS Compliance.
ATO Letter

GSA Agency FedRAMP Process
Documents
System Security Plan
Security Assessment Plan
NIST 800-53 Revision 4 Test Cases
Security Assessment Report
(Vendors) Users Guide)
Control Implementation Summary
Plan of Action and Milestones
FIPS 199 Categorization
eAuthentication Level
Rules of Behavior
(Vendors) Configuration Management Plan
(Vendors) Information System Security Policies
IT Contingency Plan
(Vendors) Incident Response Plan
Privacy Threshold Analysis and PIA

Note: The FedRAMP A&A documentation templates are available on the FedRAMP website under Documents and Templates. Please visit that website to get the current templates.

Security Reviews for Moderate Impact Software as a Service Solutions Process
Documents
IT Security Procedural Guide: Security Reviews for Moderate Impact Software as a Service (SaaS) Solutions (GSA CIO IT Security 16-71) has been developed and will be available on the GSA InSite IT Security Procedural Guides webpage when posted. Once posted, refer to it for the documents required in A&A Packages, until that time contact the OCISO for guidance. At a minimum the documentation listed below is required.
Documented results of required review activities, including:
NIST SP 800-53 SSP with a POA&M showing corrective actions for any non-implemented controls.
Implemented system and security parameters deferred to customers, i.e., the NIST SP 800-53 customer configurable controls to be implemented by GSA must be identified.
Transmissions of authentication credentials are encrypted in compliance with FIPS 140-2.
Results of their SSAE 16/SOC 2 data center certification(s) and/or show the data center(s) to

be FedRAMP certified.
Privacy Impact Assessment (PIA), approved by GSA Privacy Office.
Risk Management policies, especially business continuity information.
Web application scanning results (e.g., WebInspect, Acunetix, Burp Suite Pro, etc).
Operating System vulnerability scanning results (e.g., Nessus, Qualys, nCirlce, McAfee Vulnerability Manager, etc.).
508 compliance, or degree of compliance thereof. Concurrence must be received from GSA's Section 508 Compliance Office, as a condition of acceptance.
An acceptable flaw remediation process. Vendors must be able to identify and remediate information system flaws in a timely manner (i.e., how often scans are completed and how vulnerabilities are remediated).
Obtain an acceptable "terms of service" approved by the GSA legal office.
ATO Letter

GSA Subsystem A&A Process
Documents
FIPS 199 Low Subsystem
See Lightweight Security Authorization Process Documentation)
FIPS 199 Moderate Subsystem
System Security Plan (hybrid and system specific controls)
GSA NIST 800-53 Security Assessment Test Cases (hybrid and system specific controls)
Security Assessment Report (hybrid and system specific controls)

GSA Continuous Monitoring Program
Documents
Continuous Monitoring Plan (with all appendices) Appendix A: Software Asset Inventory Report Appendix B: Hardening Guides/Configuration baselines for each platform/software product used within the information system Appendix C: Database Configuration Scan results Appendix D: System Asset Inventory (using the inventory template) Appendix E: Hardware Asset Inventory Report generated by automated tool Appendix F: OS Vulnerability scan results Appendix G: Web Vulnerability scan results Appendix H: Code scan results Appendix I: FISMA Assessment Results Appendix J: Plan of Action and Milestones (POA&M) Appendix K: Configuration Management Plan Appendix L: IT Contingency Plan and Contingency Plan Test Results Appendix M: Incident Response Plan and Incident Response Plan Test Results Appendix N: System Security Plan Appendix O: Privacy Impact Assessment (PIA) Appendix P: Penetration Test Results Appendix Q: Self-Attestation Memo
Latest Security Assessment Report
Ongoing Security Authorization Letter

Appendix C: GSA Defined Cloud Controls

The following table contains GSA's assignment parameters for selected NIST 800-53 controls in FedRAMP's Low and Moderate baselines. These parameter settings must be used by CSPs working with GSA pursuing an authorization under the FedRAMP program. CSPs must also address the other controls in FedRAMP's baselines using FedRAMP's assignment parameters.

Table C-1. GSA Parameters for Select FedRAMP Controls

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
Account Management				
AC-2(5)	Account Management	Per GSA IT Security Policy, FIPS 199 Moderate and High impact systems shall automatically terminate a remote access connection and Internet accessible application session after 30 minutes of inactivity; 30-60 minutes for non-interactive users, long running batch jobs and other operations are not subject to this time limit. Static web sites are not subject to this requirement.	Not Applicable	AC-2(5)
AC-2(7)	Account Management	AC-2 (7 c) explicit removal actions	Not Applicable	AC-2(7)
AC-2(9)	Account Management	NA - No shared/group accounts in CMP.	Not Applicable	AC-2(9)
AC-2(12)	Account Management	Parameter 1 - Atypical times of day and originating IP address for a known privileged account user that are inconsistent with normal usage patterns. Parameter 2 - Atypical usage shall be reported to the ISSO and the GSA OCISO in agreement with GSA IT Security Procedural Guide 01-02, Incident Handling.	Not Applicable	AC-2(12)

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
AC-4(21)	Information Flow Enforcement	Parameter 1 - firewalls; host based firewalls; load balancers; subnets; DMZs; VPC, AWS Security Groups, IAM rules (for systems in AWS); to be approved by the GSA OCISO. Parameter 2 - segregation of private/system-level information systems and data from public/external information systems and data AND achievement of secure logical system specific ATO boundaries IF providing hosted platform services where hosted application require separate authorizations to operate.	Not Applicable	AC-4(21)
Security Assessment and Authorization				
CA-2(2)	Security Assessments	Parameter 1 - at least annually Parameter 2 - announced Parameter 3 - vulnerability scanning is mandatory; other activities may include in-depth monitoring; malicious user testing; insider threat assessment; performance/load testing Parameter 4 - continuous monitoring	Not Applicable	CA-2(2)
CA-2(3)	Security Assessments	Parameter 1 - FedRAMP Authorized information system Parameter 2 - Any FedRAMP Accredited 3PAO Parameter 3 - the conditions of a P-ATO in the FedRAMP Secure Repository	Not Applicable	CA-2(2)
CA-3(3)	System Interconnections	Parameter 1 - System ATO Boundary (i.e., CMP); Parameter 2 - Boundary Protections which meet Trusted Internet Connection (TIC) requirements	Not Applicable	CA-3(3)
CA-3(5)		CA-3(5) Parameter-1: deny-all, permit-by-exception Parameter-2: CMP components	Not Applicable	CA-3(5)
Configuration Management				
CM-5(3)	Access Restrictions for Change	CM-5 (3) software and firmware components	Not Applicable	CM-5(3)

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
CM-6(1)	Configuration Settings	All operating systems	Not Applicable	CM-6(1)
CM-7(5)	Least Functionality	(a) all authorized software as defined in the Software Inventory in Section 9.2 of the SSP and under CM-8, Information System Component Inventory (c) at least annually or when there is a change	Not Applicable	CM-7(5)
CM-10(1)	Software Usage Restrictions	Follow GSAIT Open Source Policy Framework	Not Applicable	CM-10(1)
Contingency Planning				
CP-9(3)	Information System Backup	All software (including but not limited to copies of the operating system and other critical information system software), as well as copies of the information system inventory (including hardware, software, and firmware components) required to return the system to an operational state.	Not Applicable	CP-9(3)
Identification and Authentication				
IA-5(3)	Authenticator Management	Parameter 1: all hardware/biometric authenticators Parameter 2: in person Parameter 3: each organization's registration authority Parameter 4: employees supervisor and ISSO	Not Applicable	IA-5(3)
IA-5(4)	Authenticator Management	Password complexity requirement are defined in IA5 (1). The idea here is the password complexity is automatically enforced at creation; if such a capability does not exist can be addressed through assessment including scanning, pen testing, and security controls assessment.	Not Applicable	IA-5(4)
IA-5(11)	Authenticator Management	U.S. Government Personal Identity Verification (PIV) card requirement for HSPD-12 compliance	IA-5(11)	IA-5(11)

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
Incident Response				
IR-9	Information Spillage Response	(b) The GSA Incident Response Team in the OCISO Organization following the reporting procedures identified in GSA IT Security Procedural Guide 01-02, Incident Handling (f) incident post mortem and updates to process, procedures, training to minimize the risk of recurrence	Not Applicable	IR-9
IR-9(1)	Information Spillage Response	The GSA Incident Response Team in the OCISO Organization	Not Applicable	IR-9(1)
IR-9(2)	Information Spillage Response	Annually as part of IR training (see IR-2).	Not Applicable	IR-9(2)
IR-9(3)	Information Spillage Response	Revert to last known backup, fail-over to alternate, new virtual instance, or alternate method to be reviewed and accepted by the OCISO.	Not Applicable	IR-9(3)
IR-9(4)	Information Spillage Response	Notification and Awareness Procedures detailing responsibilities of personnel exposed to spilled information. Procedures shall reflect relevant federal laws, directives, agency policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.	Not Applicable	IR-9(4)
Physical and Environmental Protection				
PE-13(2)	Fire Protection	NA for CMP; control is AWS responsibility	Not Applicable	PE-13(2)
System and Services Acquisition				
SA-9(4)	External Information System Services	Parameter 1: FedRAMP or Federally authorized to operate third-party service provider AND/OR documented MOU with OCISO approval. Parameter 2: All external systems where Federal information is processed or stored.	Not Applicable	SA-9(4)

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
SA-9(5)	External Information System Services	SA-9 (5) Parameter 1: information processing, information data, AND information services Parameter 2: FedRAMP-approved data centers Parameter 3: the FIPS 199 security categorization requirements for CMP.	Not Applicable	SA-9(5)
System and Communications Protection Policy and Procedures				
SC-6	Resource Priority	SC-6 Parameter: SC-6-1: additional resources Parameter: SC-6-2: priority Parameter: SC-6-3: of service provisions	SC-6	SC-6
SC-7(8)	Boundary Protection	SC-7 (8) Parameter SC-7(8)(1): outbound customer traffic Parameter SC-7(8)(2): the internet	Not Applicable	SC-7(8)
SC-7(12)	Boundary Protection	SC-7 (12) host based firewall or Intrusion prevention system (IPS); servers	Not Applicable	SC-7(12)
SC-12(3)	Cryptographic Key Establishment and Management	SC-12 (3) approved PKI Class 3 certificates or prepositioned keying material	Not Applicable	SC-12(3)
System and Information Integrity				
SI-2(3)	Flaw Remediation	(b) High-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days.	Not Applicable	SI-2(3)
SI-6	Security Functionality Verification	(a) all security functions including but not limited auditing/logging, application of security templates, GPOs (if applicable), security groups, FW rules (if applicable) to be approved by the OCISO (b) upon system startup and/or restart at least monthly (c) system administrators and security personnel (d) shuts the information system down and/or restarts the information system; notification of system administrators and security personnel	Not Applicable	SI-6

Appendix D: Scanning Frequency By A&A Process

Scanning/testing frequency by component type and A&A process are listed in the 06-30 Scanning Parameter Spreadsheet.

Questions for Mr. Gerard Badorrek
Chief Financial Officer
U.S. General Services Administration

Questions from Ranking Member
Gerald E. Connolly
Subcommittee on Government Operations

Hearing: "Army Fee Assistance Program: Part II"

---

1. The September 8, 2015 GSA Office of Inspector General Report, "Evaluation of GSA's Administration of the Army Childcare Subsidy Program (JEl 5-006)," found that "GSA periodically deleted emails from the system."
   In response to the Committee's request, the National Archives and Records Administration (NARA) submitted a letter to GSA asking for additional information on the agency's decision to delete these emails. In a November 19, 2015 response letter, GSA stated:

   > "E-mails were deleted in two circumstances: (1) no longer needed because **relevant information** was transferred to ImageNow, or (2) they were transitory in nature and not considered to be a record. E-mails were periodically deleted when the mailbox was approximately 97 percent full with the oldest e-mails deleted first.
   >
   > For the time covered by the Inspector General's report, it appears that the e-mails were either transitory or **the records contained in the e-mail** were transferred to ImageNow, the system of record."

   When you were asked, on January 6, about the incidents of deleted email you said:

   > "We did an investigation after the last hearing. The emails that were in question were transferred to the system of record, which was ImageNow. That was a system that was being used to retain documents and process documents related to child care."[2]

   There seems to be a discrepancy between your recent testimony and GSA’s response to NARA.

   a. Please confirm the total number of emails from AFA participants or providers deleted by GSA;

   Answer a.:

   - Approximately 21,000 emails relating to the Army Child Care Subsidy program were received from December 2014 to April 2015.

   - Emails that contained pertinent information relevant to a case file were uploaded to the system of record (ImageNow), including all attachments, and were then deleted from the shared Google email mailbox. Emails that were transitory in nature were deleted from the shared Google mailbox. Approximately 2,900 emails were deleted (removed from the original shared email mailbox).

b. For all deleted emails, please confirm whether the entire email or only "relevant information" was transferred to GSA's system of record, ImageNow;

Answer b.:

- If the email contained pertinent information relevant to a family's pending subsidy enrollment, the entire email was uploaded to the system of record (ImageNow), including any attachments.

c. Please describe what "relevant information" was transferred to ImageNow.

Answer c.:

- Relevant information is information pertinent to the email sender's account with Army Fee Assistance. Typically, this involved information required for processing an application including: employment and salary verification, child age and name, provider costs, and family contact information.

d. If the "relevant information" contained in the deleted email was transferred to ImageNow, how did the agency determine which portions of the email should be retained?

a. Who made this determination?

Answer d. a.:

- Staff were given verbal instructions by program management to upload entire emails to the system, if relevant information was contained in an email or in attachments.

b. Does GSA have an official policy governing the deletion of emails? If so, please provide a copy.

Answer d. b.:

- Yes, GSA has an official policy governing the deletion of emails. CIO Order 2160.2B Change 1 (attached), states in paragraph 10(b) the following:

> "... Any official records created in the GSA electronic mail system must be moved to a records management system in accordance with 36 CFR 1236.20(b). For instance, e-mail that contains or is deemed a record should be moved to a NARA-approved document management system, a shared network drive, or the user's workstation. If a

message is determined to be a record as described in the Agency's Records Disposition Schedule, users are responsible for ensuring those messages are not deleted before the expiration of the NARA-approved retention period."

2. During the January 6, 2016 hearing, when you were asked about the amount GSA spent in support of the AFA program between the September 10, 2015 hearing and December 31, 2015, you said:

> "We had approval to spend an additional $4.4 million in fiscal year 2015 ... The $4.4 million raised the projected cost for GSA for fiscal year 2015 to $8.4 million. We spent $6.7 million during fiscal year 2015, so we came in below the projection that we had provided to Army."

a. Please provide a break down, by month, of GSA's Army Fee Assistance program expenditures for FY 15?

Answer 2. a.:

- The $6.7 million of AFA program expenditures invoiced to Army for FY 15 breaks down as follows (in dollars):

FY 2015 Childcare Expenditures

October 2014	November 2014	December 2014	January 2015	February 2015	March 2015	April 2015
$179,275	$185,176	$222,196	$299,895	$562,020	$470,283	$922,448
May 2015	June 2015	July 2015	August 2015	September 2015	Total:	
$427,410	$702,629	$635,970	$713,615	$1,370,641	$6,691,561	

b. What cost-saving measures were implemented to bring about the reduced expenses?

Answer 2. b.:

- Most of the cost savings represented by the budget were due to delays in processing family actions. GSA implemented a Salesforce application in May 2015 in order to streamline processing for families and to better manage communications. GSA also made process improvements that increased operational performance.

c. What is the status of the remaining $1.7 million?

Answer 2. c.:

- GSA bills the Army based on actual expenses; therefore Army was only billed for the AFA actual cost of $6.7 million and not the earlier projected cost of $8.4 million.

Questions for the Record from Chairman Scott Perry

1. What role will USSM have assisting DHS as it transitions away from IBC and takes control of the TRIO solution?

   USSM's role is to advise agencies on lessons learned as they implement shared services. The USSM Modernization and Migration Management (M3) Playbook is a valuable compilation of best practices and lessons learned from government and industry for system modernizations in a shared environment. USSM will also continue to work with the Chief Financial Officer community to design common requirements for integrated solutions for mission support functions. As DHS defines its vision for the end state solution, these integrated standards will be the foundation for moving forward. However, it remains the responsibility of the agencies to determine the best path forward for their modernizations.

   USSM recommends that DHS leverage the M3 Playbook as it consolidates internally. USSM will continue to be available to support DHS as an independent and objective resource, as needed and appropriate.

2. What are the biggest risks DHS must identify, monitor, and mitigate to achieve financial systems modernization for the Transportation Security Administration (TSA) and the United States Coast Guard (USCG)?

   Change Management - The most difficult part of these projects is re-engineering business processes to align to the solution and then helping the users to buy into and adopt the change. Focusing on training, clarifying roles and responsibilities, establishing service level agreements, and defining overall success for the program by providing the proper attention, time, and resources is critical.

   - ○ Business Process Re-engineering needs to be the preferred method of resolving any identified gaps over modification/customization of the software. Governance structures need to support the idea of "one decision maker" for the consolidated solution.
   - ○ Sufficient communication with the stakeholder community is required to prepare them for the change and make sure they understand the value proposition.
   - ○ Leveraging the M3 Playbook to create a business and technical end state (with metrics to measure success) for the financial management function at DHS would help to create a shared vision for success.

   Program Management - DHS should adopt project management best practices such as developing a resource-loaded schedule which is used to track actual costs of various program activities.

   - ○ The value of an integrated, resource-loaded project schedule and strong schedule management discipline cannot be underestimated.
   - ○ Define roles and responsibilities of the headquarters and component organizations, and assign one responsible official for decision making.
   - ○ Define risks, mitigation strategies, and management practices critical to ensuring success.

Governance - A single accountable entity is critical as consensus management is not an effective way to make decisions and govern a large department-wide program. An expedited and integrated decision making process that addresses issues and mitigates risks is critical and must include senior officials in the agencies.

- There is great value in having an integrated, co-located program management team to lead the work activities and identify and resolve gaps, conflicts, and priorities on a daily basis.
- A single accountable entity is critical to resolve disputes and make decisions.

Scope - Project planning in the early stages is key. DHS needs to clearly define and articulate the vision for the end state solution to include the strategy and a roadmap to achieve the vision. Stakeholders at all levels should be bought into the vision.

- Importance of early stages of project planning - need to clearly define and articulate the vision for the financial management end state, to include the strategy and a roadmap to achieve the vision.
- All stakeholders need to understand the end state to ensure scope creep does not imperil the timely completion of the work within the defined budget.

Senator Thomas R. Carper
Post-Hearing Questions for the Record
Submitted to Ms. Emily Murphy

Nominations of Jeff T.H. Pon to be Director, Office of Personnel Management; Michael J. Rigas to be Deputy Director, Office of Personnel Management; and Emily W. Murphy to be Administrator, General Services Administration
Wednesday, October 18, 2017

GSA Oversight over the Old Post Office lease

1. As you know, there have been many questions about GSA's determination that the conflict of interest provisions in the lease for the Trump International Hotel are being complied with.

   During our introductory meeting, you said that no GSA political appointee had anything to do with that determination. Could you please confirm that for the record?

   Correct, no political appointee was involved in the Old Post Office lease determination.

   Will you commit to provide members of this Committee with any information needed for oversight purposes relating to this, or any other real property in GSA's portfolio? .

   Yes, if confirmed I look forward to working with this Committee.

Presidential Transition

2. GSA plays a critical role in presidential transitions by providing space to transition teams and the president-elect, and by playing a key role in the coordination of transition activities across the government.

   What will you do to gather lessons learned on GSA's role in the 2016 transition and to build on that experience to ensure that the next transition goes smoothly?

   If confirmed, I will ensure that GSA continues to comply with the Presidential Transition Act of 1963 and the Edward 'Ted' Kaufman and Michael Leavitt Presidential Transitions Improvements Act of 2015. It is my understanding that GSA captures lessons learned during every Presidential Transition and utilizes those lessons to improve processes and procedures for future transitions. This will require collaboration with federal partners, transition teams, and subject matter experts to compile lessons learned and identify new challenges. If confirmed, I would like to task the prior Federal Transition Coordinator to lead this effort.

Senator Steve Daines
Post-Hearing Questions for the Record
Submitted to Ms. Emily Murphy

Nominations of Jeff T.H. Pon to be Director, Office of Personnel Management; Michael J. Rigas to be Deputy Director, Office of Personnel Management; and Emily W. Murphy to be Administrator, General Services Administration
Wednesday, October 18, 2017

1. In 2013, GSA sold the old Batten Courthouse in Billings, MT to a buyer that by all counts didn't have the ability to make good on its over $2.2 million loan. Sure enough, the buyer made no payments, and the asbestos filled building nearly transferred to the local government's ownership as both a financial and health liability. How would you change GSA's disposal policy to ensure only creditworthy buyers can purchase buildings with health hazards? If confirmed, will you ensure that GSA will work with my staff to draft a bill to make the situation in Billings doesn't happen again?

   Yes, if confirmed, I pledge to work with you and your staff and GSA's Public Buildings Service, to identify areas to improve the disposal process and public sale of unused and underutilized real property.

2. If you are confirmed, how would you standardize GSA practices and policies so that contracting officers apply these practices and policies in a consistent, even-handed manner? How should federal contractors who believe they are being treated less favorably than their competitors by their contracting officers escalate the problem to GSA Management?

   If confirmed, I will strengthen the Procurement Management Review process in order to standardize GSA practices and policies to ensure that contracting officers apply federal statutes and regulations evenhandedly and in full compliance. I will ensure that policies are clarified and training enhanced. Further, when federal contractors believe they are being treated less favorably than their competitors, they should avail themselves of GSA's Office of the Procurement Ombudsman, the GSA Competition Advocate, or the GSA Office of Small Business Utilization. Each of these offices has the ability to appropriately escalate issues, while avoiding the issues identified by the Office of the Inspector General in Report Number A120161/Q/6/P13003, that identified some inappropriate management intervention in procurement in 2013.

3. How do you plan to address the issue of delays caused by an excessive focus on catalog-level pricing? What is your position on order-level pricing, and increased competition at the order-level?

   If confirmed, as part of my focus on reducing duplication, I would like to use systems modernization and process reengineering to speed the initial contract award for GSA's

Multiple Award Schedules program. I support increased competition at the task order level on multiple award contracts, and believe contracts like the OASIS Small Business contract demonstrate the value of increasing task order level competition, especially in areas where the statement of work may substantially vary between task orders.

Senator Kamala Harris
Post-Hearing Questions for the Record
Submitted to Ms. Emily Murphy

Nominations of Jeff T.H. Pon to be Director, Office of Personnel Management; Michael J. Rigas to be Deputy Director, Office of Personnel Management; and Emily W. Murphy to be Administrator, General Services Administration
Wednesday, October 18, 2017

Calexico West Land Port of Entry Project

The current Calexico West Port of Entry (POE) was constructed in 1974. It is outdated and badly in need of updating. Wait times for passenger vehicles and pedestrian crossers at the Calexico West POE cost Imperial County and the State of California jobs, economic activity, and tax revenue.

1. The GSA listed the Calexico West Port of Entry project as a priority on its new construction list in the GSA's proposed FY17 budget. The project was removed as a priority from the new construction list in GSA's FY18 budget proposal. Will you consider reiterating the importance of the project to appropriators by adding the project to the list of new construction priorities in GSA's FY19 budget proposal or through a budget addendum to the FY18 budget proposal?

   It is my understanding that the Calexico West LPOE is a priority for GSA, and that Phase I of this project is scheduled for completion in 2018. I further understand that GSA requested funding for Phase II in FY17, but this was not funded by Congress. If confirmed, I am committed to working with you and GSA's partner agencies to seek the funding to complete this project.

Transfer of GSA-managed Property to City and County of San Francisco for Permanent Supportive Housing for the Homeless

The City and County of San Francisco is in the process to acquire and develop surplus property managed by GSA to provide permanent supportive housing for chronically homeless individuals.

1. If confirmed, will you commit to help ensure the speedy completion of this transfer?

   Yes, if confirmed, I look forward to working with you and your staff on this important project.

2. What are your views on repurposing or transferring unused GSA-managed properties to state and local partners when there is a clear public benefit?

I support Public Benefit Conveyances and the role they play in assisting GSA in removing properties from its portfolio and transferring them to state and local entities that will utilize them for a public benefit.

3. If you are confirmed, will you commit to getting my office an assessment of all unused federal sites in California?

   Yes, if confirmed I look forward to working with you and your staff to provide this information.

Senator Heidi Heitkamp
Post-Hearing Questions for the Record
Submitted to Ms. Emily Murphy

Nominations of Jeff T.H. Pon to be Director, Office of Personnel Management; Michael J. Rigas to be Deputy Director, Office of Personnel Management; and Emily W. Murphy to be Administrator, General Services Administration
Wednesday, October 18, 2017

1. In your opening statement, you mentioned shared services as a strategy you support for helping agencies reduce duplication in government activities.

    a. Please elaborate on the current state of the shared services initiative, including the role, authorities and resources levels of GSA's Office of Unified Shared Services Management (USSM), recent implementation progress, and any changes you anticipate in the way shared services are being implemented by the Trump Administration.

    The Unified Shared Service Management (USSM) office was created within the General Services Administration in 2015 to design the standards for more integrated solutions of administrative functions across lines of business, provide transparency into the performance of Federal Shared Service Providers to inform agency decision making, and to provide advice and guidance to agencies who are planning for the acquisition of new administrative solutions based on lessons learned and best practices. USSM's mission is to transform the way government does business internally to improve the way the government serves the American public.

    Today, USSM is staffed with seven people and the President's budget proposes a $2 million appropriation to support the identification and prioritization of work that can be shared across government. USSM does not have the authority to direct agencies to move to shared services; however, USSM is a source of best practices, tools, and lessons learned to help guide agencies through the process of adopting a service provided by either a Federal or commercial provider. If confirmed, I would like to coordinate with Congress and OMB to explore the opportunity for GSA to take a leadership role in evaluating business cases for shared services.

    b. What do you see as the major barriers to shared services expansion, and how do you intend to address them?

I believe that one of the key barriers to the adoption of shared services has been the failure to accurately articulate requirements in a coordinated and consistent way across government. Additionally, in the areas where the government has moved to shared services, it invested in systems without planning for transition, and failed to leverage best practices and processes for managing the change within their organizations.

If confirmed, to address these problems, I would promote the USSM methodology and governance structure to drive requirements definition, and to work with the Federal community to agree on standard business rules for common functions. To address the issue of transition cost, I would like to work with Congress on approaches like the Technology Modernization Fund to help move agencies from legacy systems to shared services, and to ensure that new shared services contemplate funding transition costs at the time of initial award. For example, in the area of telecommunications, the Networx contract vehicle addressed transition to the ultimate successor contract when it was initially awarded ten years ago, which will make the transition to Enterprise Infrastructure Solutions (EIS) possible.

c. Does USSM have sufficient authority and resources to perform the role you envision?

To drive real change in the sharing of administrative services across the Federal Government, it will require continued leadership from both Congress and the Administration. Leveraging this strong leadership, I believe USSM has sufficient resources and authorities to move the program forward, but would welcome the opportunity to work with you on potential future reforms.

2. Since 2003, management and divestment of Federal real property has been a repeat offender on GAO's "High-Risk List". Regarding the disposal of excess and underutilized real property, GAO has identified a lack of reliable data, complex disposal processes, costly requirements, competing interests and limited accessibility as hurdles to a more expedient disposal process.

a. In your opinion, what can GSA do to encourage agencies to dispose of underutilized properties and what can Congress do to expedite the disposal process?

If confirmed, I will work with the Public Building Reform Board and the Federal Real Property Council to identify unused and underutilized properties, and then to expedite the disposal of these properties. I will also work with our tenant agencies to examine how we can reduce their real property footprint by identifying areas for consolidation and disposal. It is my understanding that over 100 million square feet of GSA leases will expire in the next five years. This creates an opportunity to collaborate with Congress and agencies to consolidate operations, but it will require frank discussions about agency requirements. Likewise, if confirmed, I would explore opportunities to use these expiring leases to save taxpayer money, either by reducing reliance on short term leases or by analyzing opportunities for ground lease leasebacks or discounted purchase options.

Given that the new expedited disposal authorities were provided by Congress as part of the Federal Assets Sale and Transfer Act of 2016 and the Federal Property Reform Act of 2016 but have not yet been used, I would like to have the opportunity to assess how well these work, and then work with Congress if additional reforms are necessary.

b. With the many responsibilities as a Director, if confirmed, what issues will be top priority?

If confirmed, in the area of real property, one of my priorities is to improve access, transparency and data quality in the FRPP. By having a better understanding of what the government owns or leases, we can better manage these properties. In addition, I plan to work closely with OMB and the Public Buildings Reform Board when it is established to identify underutilized property and either consolidate or dispose of these assets. Finally, at the suggestion of Senator Carper, if confirmed I will request a standing meeting with GAO to focus on the outstanding risk list items.

3. A significant challenge faced by agencies in the divestment and management of Real Property assets is the cost of maintenance and environmental remediation activities. On many occasions, GAO has found that the cost to agencies in deferred maintenance and/or legal requirements, such as the preservation of historic properties is higher than potential proceeds from sale of the property.

a. Based on these findings, what actions can GSA take to aid agencies in mitigating these challenges associated with Real Property Management and disposal?

If confirmed, I am committed to utilizing all the tools available to GSA, including new authorities provided by FASTA to reduce the Federal Government's real property footprint.

Ranking Member Claire McCaskill
Post-Hearing Questions for the Record
Submitted to Ms. Emily Murphy

Nominations of Jeff T.H. Pon to be Director, Office of Personnel Management; Michael J. Rigas to be Deputy Director, Office of Personnel Management; and Emily W. Murphy to be Administrator, General Services Administration
Wednesday, October 18, 2017

COOPERATION WITH CONGRESS

Q: Do you agree that FOIA exemptions do not apply to congressional oversight requests?

Yes.

Q: Will you pledge to copy the Ranking Member and/or staff on all official correspondence with the Committee and ensure that such correspondence is transmitted to the Ranking Member's office contemporaneous with transmittal to the Committee?

Yes.

Q: Will you pledge to ensure that all meetings, briefings, and other official engagements with the Committee staff include both the majority and minority?

Yes.

WHISTLEBLOWER PROTECTION

Q: What specific steps will you take to promote a culture where employees can raise concerns to senior management, including directly to you?

I take seriously the charge to uphold the highest ethical standards. As I said in my testimony before the committee at my nomination hearing, the first overarching principle I will pursue if confirmed is "to provide ethical leadership" at GSA. The Office of Government Ethics recently sent a letter reminding us that "the citizens we serve deserve to have confidence in the integrity of their Government [but the] public's trust is not guaranteed." I will strive to earn that trust every day, by creating a culture within GSA that puts the taxpayer first, encourages a diversity of opinions, values the contributions all employees, and promotes a safe culture for reporting misconduct.

Recently, the GSA Inspector General cited the former GSA Administrator for retaliating against a whistleblower regarding potential changes to the agency's Technology Transformation Service.

Q: Describe what steps you have taken and will take to address the IG's report and to prevent retaliation against whistleblowers at GSA.

As I stated in my policy questionnaire, I am well aware of how difficult it can be for individuals to step forward, but also of how crucial it is that they do so. Since returning to GSA earlier this year, I worked to quadruple the ethics training provided to political appointees, and coordinated training for all appointees with the Inspector General. If confirmed, I will work with the Inspector General, and the Office of Special Counsel to ensure that GSA cooperates fully with any investigation, and to create an environment where all employees and contractors are encouraged to report waste, fraud and abuse.

ACQUISITION REFORM

Q: What actions should GSA take to improve outreach to the contractor community to ensure that qualified veteran-owned, minority-owned, women-owned, rural, HUBZone and other small businesses compete for contracts?

If confirmed, I would work with the Small Business Administration, Small Business Procurement Advisory Council, Procurement Technical Assistance Centers, Small Business Development Centers, trade associations, and other third parties to ensure that small businesses, veteran-owned small businesses, service-disabled veteran-owned small businesses, woman-owned small businesses, economically-disadvantaged woman-owned small businesses, HUBZone business enterprises, rural businesses, 8(a) small businesses, and small disadvantaged businesses are: (1) better educated on the opportunities to compete for federal contracts; (2) easily identified on GSA contract vehicles. Further, I will continue the work on making the GSA solicitations more accessible to small businesses by adopting plain language. Finally, I will work to make sure that new contract vehicles are designed to maximize competition, both at the contract and task order level, which will create more opportunities for these businesses.

BOLSTERING INFORMATION TECHNOLOGY AND CYBER SECURITY

The Government Accountability Office (GAO) has extensively reported on the need for the federal government to reduce its reliance on legacy information technology systems. According to a 2016 GAO report, some agencies are still using decades-old IT systems. This failure to modernize not only undermines the efficiency of federal agencies but also poses serious cyber-security risks to sensitive national security and other government data.

Q: If confirmed, what changes should GSA implement to assist its sister agencies in reducing their reliance on legacy IT systems?

If confirmed, I hope to build upon the work GSA is doing to help Federal agencies reduce their reliance on legacy IT systems. First, I would do this by ensuring that contract and service offerings look to the future and provide enhanced security, efficiency, and ease to continue modernizing as technology evolves. For example, currently GSA is transitioning agencies from the legacy Networx contract, under which agencies purchased $1.79 billion in network and telecommunications services in FY 2016, to a comprehensive solution-based contract vehicle called Enterprise Infrastructure Solutions (EIS). Second, pursuant to the Office of Management and Budget (OMB) M-16-19, I would support the roles assigned to GSA's Office of Government-wide Policy (OGP) serves "as the managing partner of the Federal Government's data center line of business and data center shared services." Third, I hope to use the expertise within the Federal Acquisition Service's Technology Transformation Service (TTS) to assist agencies through a variety offerings to best achieve their missions with modern technology. For example, components of TTS have an expertise in agile acquisition, cloud migration, and identity verification. Fourth, if Congress chooses to pass the Modernizing Government Technology (MGT) Act, I would look forward to using these new tools to partner with other agencies on modernization. Finally, over the years I have found that IT modernization is frequently inhibited due to regulations that are outdated and serve as barriers to entry for innovative companies, so,if confirmed, I would direct GSA, as a member of the Federal Acquisition Council, to work alongside with the Office of Federal Procurement Policy, DOD, and NASA to review regulations that restrict modernization efforts.

FEDERAL REAL PROPERTY

The Government Accountability Office has included federal real property management on its list of High Risk programs each year since 2003. This period has included three administrations and spanned the tenure of several GSA Administrators.

Q: GSA is the primary agency responsible for addressing this high risk area. If confirmed, do you have confidence that you will be able to move federal real property management off GAO's High Risk list? How will you accomplish this goal?

One way to address some of the issues on the GAO High Risk list is to utilize new authorities provided in the FAST Act. The legislation has given the Federal Government an opportunity to improve its management of real property and identify savings for the American taxpayer by incentivizing the more effective use of real property. GSA has already begun outreach to other Executive branch agencies and collected real property data to enable the Public Buildings Reform Board to make smart real estate decisions.

VOTER INTEGRITY COMMISSION

On May 11, 2017, the President issued a Presidential Executive Order on the Establishment of a Presidential Advisory Commission on Election Integrity. The Executive Order states that "to the extent permitted by law, and subject to available appropriations, the General Services Administration shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis." You acknowledged in your policy questionnaire that GSA does, in fact, provide administrative support to the Commission on a reimbursable basis.

Q: What specific administrative services has GSA provided to the Commission to date?

GSA has supported the Commission with travel arrangements, complying with Federal Advisory Committee Act requirements, assisting with the purchase of voter data from States, and purchasing of live web streaming services for Commission meetings.

Q: What administrative services provided by GSA to the Commission are anticipated in the future?

GSA anticipates similar support services to the Commission in the future.

Q: What specific GSA facilities has the Commission utilized to date?

The Commission has not utilized GSA space or facilities.

Q: What GSA facilities are anticipated to be used by the Commission in the future?

To date, the Commission has not communicated any current or future needs for GSA facilities.

Q: What specific GSA equipment and other support services has the Commission utilized to date?

No GSA equipment has been provided to the Commission. GSA has supported the Commission with travel arrangements, complying with Federal Advisory Committee Act requirements, assisting with the purchase of voter data from States, and purchasing of live web streaming services for Commission meetings.

Q: What specific GSA equipment and other support services are anticipated to be used by the Commission in the future?

GSA does not anticipate any equipment use requests from the Commission and anticipates similar support services to the Commission in the future.

Q: What is the total dollar amount of all GSA funding that has been expended to date to support the Election Integrity Commission?

GSA has not utilized any GSA funds to support the Commission.

Q: What is the total dollar amount of anticipated GSA funding expended to support the activities of the Commission?

GSA does not anticipate any GSA funds to be expended in support of the Commission.

Q: What is the total dollar amount of reimbursements that GSA has received to date from the Commission?

Thus far, GSA received $85,000 in reimbursements from the Office of the Vice President for support provided to the Commission.

Q: What is the funding source for all reimbursements GSA has received to date from the Commission?

GSA entered into an interagency agreement with the Office of the Vice President for reimbursement of GSA support to the Commission.

Q: How many GSA employees have staffed the Commission to date?

GSA has dedicated portions of five (5) individuals’ time to support the Commission.

Q: Are there additional resources that GSA anticipates providing the Commission in the future?

No.

Q: What, if any, guidance or training has GSA given its employees staffing the Commission in terms of recordkeeping practices that comply with the Federal Records Act and Presidential Records Act?

GSA provided individuals within GSA supporting the Commission guidance on time and record keeping.

Q: What, if any, instructions have GSA employees staffing the Commission received regarding the use of private email accounts for official Commission business?

GSA provides all employees, including those supporting the Commission, with training on the use of private emails.

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2160.2B CHGE 1
June 17, 2015

GSA ORDER

SUBJECT: GSA Electronic Messaging and Related Services

1. Purpose. This Order updates GSA's directive on electronic messaging due to the move from a server-based messaging system to cloud-based e-mail and collaboration tools and additional federal requirements for managing electronic mail records. This directive addresses security, appropriate use, and recordkeeping of the GSA Enterprise Messaging Services (GEMS) in a cloud-based environment.

2. Cancellation. This Order cancels CIO 2160.2A.

3. Applicability. This Order applies to all authorized users who are granted access to GEMS and to all communications sent or received via GEMS.

4. Directive. All authorized users must comply with Federal laws and regulations relative to GEMS use, which are listed in Appendix A, References. The misuse of GEMS by authorized users can severely hamper the Agency's ability to conduct business and accomplish its mission. It is essential that users learn how to use electronic mail and collaborative tools efficiently, effectively, and courteously, practicing good security, records management, and using e-mail in a responsible, professional, and lawful manner. Additionally, users have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses. The Agency reserves the right to limit authorized users' electronic messaging access following evidence that shows prohibited or inappropriate use of the system or such use that creates an appearance of impropriety in the public view. Prohibited use is that which is forbidden by, or fails to comply with Federal laws, regulations or GSA directives.

5. Reporting violations. All suspected violations of Federal laws and regulations relative to GEMS use; such as, security or privacy breaches, violations of Agency policy, malicious or otherwise prohibited use, shall be reported to the Information System Security Officer (ISSO) and/or Information System Security Manager (ISSM). ISSOs/ISSMs must report security incidents to the GSA Senior Agency Information Security Officer (SAISO) in accordance with CIO Procedural Guide 01-02, “Security Incident Handling.” The SAISO will determine which security incidents should be reported to the United States Computer Emergency Readiness Team (US-CERT). The SAISO also will report incidents to the GSA Office of Inspector General

(OIG) in accordance with CIO Procedural Guide 01-02. All incidents involving Personally Identifiable Information must be reported to the OSAISO within one hour of discovering the incident. There should be no distinction between suspected and confirmed breaches. Anyone needing assistance in determining whether a violation has occurred may contact their local ISSO/ISSM for assistance. For ISSO, ISSM and OSAISO points of contact go http://insite.gsa.gov/graphics/staffoffices/poc.xls.

6. E-mail accounts and files.

a. E-mail account. An account is established between an authorized user and GEMS for the purpose of creating, sending, and receiving electronic mail messages. E-mail accounts are accessed using your GSA Active Directory Credentials.

(1) GSA provides annual security training for authorized users to take at the initiation of their account and to be taken annually thereafter. Any authorized user of GEMS who fails to complete the annual GSA security training will have their e-mail account disabled. Accounts will be reinstated upon verification of the completion of the annual security training.

(2) System administrators, responsible for continued operation, maintenance, availability and accessibility of assigned system(s), will monitor all e-mail accounts for indication of inactivity. An "inactivity warning" notification will be sent to the user of any e-mail account not accessed in a 30-day period and to designated points of contact. If an e-mail account has not been accessed in a 45-day period, the e-mail account will be considered "inactive" and the e-mail account suspended. Any e-mail account that has not been accessed in a 60-day period will be terminated.

b. E-mail and related functionality.

(1) An Active Directory Account is required to access an e-mail account and related functionality within a limited storage space capacity. An individual e-mail account consists of an Inbox, Sent, Trash and other user-created folders for use in the creation, sending, receiving and organization of electronic mail messages, attachments, user-saved instant messages, and Mp3 voicemail messages received through the Voice over Internet Protocol (VoIP) telephone integration. Additional features of GEMS include calendaring, instant messaging, and collaboration tools for sharing documents, spreadsheets, presentations, and drawings.

(2) A single archive repository stores all inbound and outbound email messages and their attachments sent or received through the gsa.gov domain for e-discovery purposes for an indefinite period of time. The archive repository will also be used for indefinite storage of litigation hold information.

(3) All messages and their associated attachments sent and received will be scanned for viruses. Messages containing viruses will be cleaned and forwarded to the

intended recipient(s) electronically. If a message is unable to be cleaned, that message will be quarantined and not forwarded.

(4) Messages larger than 25 megabytes (MB) will not be sent or received.

7. Electronic message control.

a. Message privacy. GSA provides electronic messaging services to authorized users, at GSA expense, for their use on GSA or other Government business. All electronic communications sent or received are owned by the Federal Government. The Agency may access any message sent over its electronic services for a legitimate Governmental purpose. Occasional personal use of the electronic services that involves minimal expense to the Government, does not interfere with Government business, and otherwise conforms to GSA's personal use policy is authorized. However, authorized users have no expectation of privacy with regard to electronic messages, official or personal, sent through the Government-provided electronic messaging services.

b. Monitoring.

(1) Obtaining access to GSA resources constitutes acknowledgment that monitoring activities may be conducted.

(2) Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring.

(3) GSA performs electronic monitoring of e-mail messages transmitted out of the GEMS environment for leakage of Personally Identifiable Information (PII) and/or sensitive data (e.g., Social Security Numbers, Credit Card Numbers, etc.) without required encryption as stipulated in paragraph 7.c.

(4) In the performance of their duties to ensure system reliability, the GEMS system administrators/managers regularly monitor the efficient functioning of electronic messaging services, not the content of messages. These system administrators/managers review the system logs created by the various electronic messaging services to analyze service delivery problems. The logs usually contain information about each message, including sender address, receiver address, size of message, and date and time of day, but not the content of the message. These logs are retained locally for 14 days and then destroyed, if they are not being used for problem analysis. System administrators/managers only open e-mail messages and review their content when attempting to locate a message, pursuant to a request by an approved official or an OIG investigator.

(5) If system administrators/managers find indications of illegal activity, violations of Agency policy or security, they will report their findings to the appropriate ISSO/ISSM. ISSO/ISSMs must report security incidents to the OCIO SAISO in

accordance with CIO Procedural Guide 01-02. The SAISO will report incidents to the OIG in accordance with that Procedural Guide. All incidents involving PII must be reported to the OSAISO within one hour of discovering the incident. There should be no distinction between suspected and confirmed breaches. Any incident which involves PII and could result in identify theft must be handled in accordance with the procedures outlined in GSA Order CIO P 2100.1G.

(6) Supervisors may request the review of the electronic messages of anyone they supervise, if they have reason to suspect there has been any breach of security, violations of GSA policy or other misconduct on the part of the associate. This may include inspection of the contents of electronic messages disclosed in the course of such monitoring or any follow up inquiry, if necessary to serve an official purpose. The supervisor will be required to explain the need to gain access to the suspected individual's message files in writing along with the purpose for seeking access to the content of the individual's messages. The request must go to the GSA Office of the CIO GEMS management. The next level of authority to whom the requesting supervisor reports within GSA, if any, will instruct or authorize further steps and actions based upon findings of the request and seek the advice of the General Counsel and Chief People Officer.

(7) It is a misuse of Federal Government time and resources and a violation of this directive for anyone, including system administrators, managers, and supervisors, to peruse electronic mail or other electronic messages, or use Agency computer systems in any fashion to satisfy idle curiosity about the affairs of others, with no business purpose for obtaining access to the files or communications of others. Anyone engaging in "snooping" is subject to disciplinary action, up to and including removal.

c. Message encryption. Message encryption is the use of software to render a message unreadable to everyone except the sender and its intended recipient. Users shall send external E-mail messages including sensitive information, such as PII, procurement sensitive information, etc., as deemed by the data owner, with GSA provided encryption that uses certified encryption modules in accordance with FIPS PUB 140-2, “Security requirements for Cryptographic Modules,” or using WINZIP with FIPS-197 certified Advanced Encryption Standard (AES).

d. Disclosure.

(1) Electronic messages may be treated as Agency records for purposes of the Freedom of Information Act, 5 U.S.C. § 552 and the Privacy Act, 5 U.S.C. § 552a. As such, electronic messages or portions of them may be required to be disclosed upon a proper request. Additionally, they may be disclosed pursuant to discovery in a legal proceeding or upon request by Congress. The contents of electronic messages, properly obtained for Federal Government purposes, may be disclosed within the Agency for an official purpose without the permission of the authorized user who created the message. Whenever practicable, however, the author of the message will be informed regarding further dissemination of the message.

(2) The Agency may disclose information regarding the number, sender, recipient and addresses of electronic communications sent over the electronic messaging services as authorized by law.

8. Appropriate use.

a. When using GEMS, users are doing so as employees and/or representatives of GSA and the Federal Government. Users should at all times seek to promote a positive image for GSA and the Federal Government. They should be careful about how they represent themselves, given that what they say or do could be interpreted as GSA or Federal Government opinion. Users should be aware that their conduct could reflect on the reputation of GSA, the Federal Government, and its associates.

b. All users have an obligation to learn about e-mail etiquette, customs, and courtesies. Certain procedures and guidelines should be followed when using electronic mail communications, participating in electronic mail discussion groups, and sending attachments.

c. All users have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses. Users who load files brought in from outside sources on Federal Government computers, then send the files as e-mail attachments, present a heightened risk in this area, unless the users first virus-scan all outgoing attachments before the e-mail is sent out. Always exercise caution when addressing e-mail messages, as there are users of the Agency's services who are not Agency associates. This will help to avoid inadvertently sending a message meant for GSA associates and authorized users to outsiders. Finally, never use e-mail for transmitting or storing classified data.

d. Users must exercise caution in conveying sensitive or non-public information. Such information should be treated with the same care as paper documents conveying the same information. Sensitive information is that which would be withheld from disclosure under Privacy Act, the Freedom of Information Act, procurement-sensitive information, proprietary information of GSA service partners and suppliers, or other information deemed sensitive by the Agency.

9. Inappropriate use.

a. Conveying of classified data or information. Users shall never convey classified data or information in any messages sent over the GSA electronic mail system.

b. Unlawful or malicious activities are prohibited. The activities include, but are not limited to:

(1) Use of offensive, abusive, discriminatory or objectionable language or graphics in either public or private messages;

(2) Use of lewd or sexually explicit language or graphics that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit materials, or materials or remarks that ridicule others on the basis of race, creed, religion, color, sex, handicap, national origin, or sexual orientation;

(3) Using GEMS to misrepresent oneself, GSA, or the Federal Government;

(4) Using GEMS to "snoop" on or invade another person's privacy merely to satisfy idle curiosity and with no legitimate Federal Governmental purpose;

(5) Any use that reflects adversely on GSA or the Federal Government;

(6) Transmitting any material pertaining to GSA, the Federal Government, or any agency employee or official that is libelous or defamatory; and

(7) Automatically forwarding E-mail messages from GSA E-mail addresses to any non-Federal E-mail account(s) or addresses.

c. <u>Malicious use and denial of service</u>. Unlawful or malicious activities that would result in a denial of service to other users and abuse of resources are prohibited. Malicious Use is designed to embarrass, harm or otherwise cause others to suffer. Denial of service is one type of malicious use. Denial of service is any activity that interferes with official GSA or Federal Government business by overloading resources, or blocking access to any resources. Abuse of resources is use that results in no benefit to GSA or the Government, and causes the Agency additional expenses through increased load on networks, systems and staff. Examples are transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, unauthorized mass mailings, or intentionally sending a virus/worm.

d. <u>Abuse of resources</u>. Abuse of resources refers to any use of Federal Government time or resources that results in no benefit to the Federal Government. Examples include but are not limited to:

(1) Joining electronic discussion groups (listservs, newsgroups, etc.) that are not Federal Government business-related and result in mailings to an authorized user at work;

(2) Any use for an authorized user's own private gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives or persons with whom the authorized user is affiliated in a nongovernmental capacity, including nonprofit organizations of which the authorized user is an officer or member, and persons with whom the authorized user has, or seeks, employment or business relations; and

(3) The use of the electronic messaging services to solicit Agency authorized users for any purpose not related to official Federal Government business.

e. Inappropriate signature block content. The signature block is the part of an e-mail message that contains the sender's contact information. This information usually consists of at least the sender's name and phone number. A signature block might also include additional information, such as job title, department/organization, mailing/office address, e-mail address, fax or cell phone numbers, business web site address, business slogan, etc. A signature block is typically located at the end of an e-mail message. Signature blocks are intended to be used as a method of providing sender contact information to message recipients. Only GSA and GSA business-related slogans may be used as part of a message signature block. In addition, use of graphics in the signature block should be limited and is restricted to GSA and GSA business-related logos, such as the GSA logo/seal.

10. Record keeping of e-mail messages.

a. E-mail recordkeeping is governed by National Archives and Records Administration (NARA) directives. Authorized users are responsible for maintaining their files within assigned storage limitations and NARA records management requirements. Authorized users are advised to apply the same decision-making process to e-mail for records maintenance and disposition that they apply to other documentary materials, regardless of the media used to create them, and store them accordingly.

b. The GSA electronic mail system is not an authorized official records storage system for GSA records management purposes. Any official records created in the GSA electronic mail system must be moved to a records management system in accordance with 36 CFR 1236.20(b). For instance, e-mail that contains or is deemed a record should be moved to a NARA-approved document management system, a shared network drive, or the user's workstation. If a message is determined to be a record as described in the Agency’s Records Disposition Schedule, users are responsible for ensuring those messages are not deleted before the expiration of the NARA-approved retention period.

c. Non-record material (transitory documents, copies, and drafts) may be retained in an e-mail file indefinitely in accordance with 36 CFR 1236.22. Authorized users are responsible for reviewing their e-mail regularly and for deleting all such material as soon as it has served its purpose. Transitory refers to documents of short-term interest having no documentary or evidential value and which normally need not be kept indefinitely. Examples of transitory material are:

(1) Routine requests for information or publications and copies of replies that require no administrative action, no directive decision and no special compilation or research for reply. Freedom of Information requests are not considered transitory material;

(2) Originating office copies of letters of transmittal that do not add any information to that contained in the transmitted material, and the receiving office copy, filed separately from transmitted material;

(3) Quasi-official notices, including memoranda and other records, that do not serve as the basis of official actions, such as notices of holidays or charity and welfare fund appeals, bond campaigns and similar correspondence;

(4) Copies of documents issued to multiple recipients. Usually, copies of documents received by recipients of e-mail are copies, not records, and should be thrown away as soon as they are not needed for reference. However, multiple copies of the same document may meet the definition of records, if any copy is used by the recipient to transact Agency business. Copies that have such record status are usually filed in different record-keeping systems and are used for different purposes;

(5) Drafts circulated for comment. In general, draft copies are not records. However, draft documents or working papers that propose or evaluate high-level policies or decisions and provide unique information that contribute to the understanding of major decisions, must be preserved as Federal records, whether they are in printed or e-mail form;

(6) Extraneous copies of records used or issued to conduct or transact official business. Normally, only the originator copy is the record copy.

(7) User-saved instant messages and Mp3 voicemail messages.

11. Waivers. Request for waivers to this order must be submitted to the GSA Chief Information Officer for review and approval.

12. Explanation of change paragraph. The change in retention period for emails from 180 days to “indefinite” is due to upcoming changes that will align GSA policies to NARA's Capstone approach.

13. Signature.

/S/______________________________
DAVID SHIVE
Acting Chief Information Officer
Office of GSA IT

Appendix A. References

1. Federal Laws & Regulations.

5 U.S.C. § 552, the Freedom of Information Act

5 U.S.C. § 552A, the Privacy Act

44 U.S.C.§ 2901 *et sec.*, the Federal Records Act

44 U.S.C § 3301, the Federal Records Disposal Act

17 U.S.C. § 101 *et sec.,* the Copyright Act of 1976

Public Law 99-474, The Computer Fraud and Abuse Act of 1986

18 U.S.C. § 798, AND 50 U.S.C. § 783(b) regarding protection of Classified Information

18 U.S.C. § 1905, Which prohibits disclosure of proprietary information and certain other confidential information

41 U.S.C. § 423(a), which prohibits unauthorized disclosure of certain procurement-sensitive information, including proprietary or source selection information

5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch, particularly subpart G which deals with misuse of position

36 C.F.R. Parts 1220, 1222, 1228 and 1234, 1236, National Archives and Records Administration regulations on management of e-mail messages

FIPS PUB -140-2 Security Requirements for Cryptographic Modules

FIPS PUB -197 Advanced Encryption Standard (AES)

2. Agency Directives.

GSA IT Security Policy, GSA Order CIO P 2100.1I

GSA IT Security Procedural Guide: Incident Response (IR)-CIO IT Security 01-102

Personal Use of Agency Office Equipment, GSA Order ADM 7800.11A